Cabletron Systems ISDN Router

CSX100 Series

User Guide

First Edition (September 1998)

Published by:

Cabletron Systems
35 Industrial Way
Rochester, NH 03867
U.S.A.

Internet Web Site: http://www.cabletron.com

P/N 222-00499-01

Software License Agreement and Warranties

SOFTWARE LICENSE AGREEMENT AND WARRANTIES

License Agreement

This product contains certain Software (computer programs, firmware and media) the use of which are subject to this license agreement. If you do not agree with all the terms, you must return this product, all manuals and documentation, and proof of payments, to the place you obtained them for a full refund within 30 days of first acquiring this product. Your written approval is not prerequisite to the validity or enforceability of this agreement and no solicitation of any such written approval by or on behalf of Cabletron Systems shall be construed as an inference to the contrary.

License and Term

Cabletron Systems and any applicable sublicensors grant to you a non-exclusive, non-transferable license to use the Cabletron Systems software programs and related documentation in this package (collectively referred to as the "Software") on one licensed router. If the Cabletron Systems product that you acquired is an upgrade, then the terms and conditions of this agreement apply equally to the upgraded product. Any attempted sublicense, assignment, rental, sale or other transfer of the Software or the rights or obligations of this Agreement without the prior written consent of Cabletron Systems shall be null and void. You agree not to export or re-export this product without prior authorization from the U.S. and other applicable government authorities. This License will automatically terminate without notice to you if you fail to comply with its terms. This Agreement will be covered by the laws of the State of California.

The Software and documentation are copyrighted. You may make copies of the Software only for backup and archival purposes. Unauthorized copying, reverse engineering, decompiling, disassembling, and creating derivative works based on the Software are prohibited. Title to the Software is not transferred to you by this license. Ownership and title to the Software and to the actual contents of this package, including the copy of the Software and the media on which it is stored and the associated documentation are retained by Cabletron Systems and/or its licensors.

U.S. Government End Users. The [Licensed Product] is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (OCT 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and is provided to the U.S. Government only as a commercial end item. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (JUNE 1995), all U.S. Government End Users acquire the [Licensed Product] with only those rights set forth herein.

Limited Warranty on Media and Damages Disclaimer

Cabletron Systems or its distributors or resellers will repair or replace free of charge any defective recording medium on which the Software is recorded if the medium is returned to Cabletron Systems or its distributor or reseller within ninety (90) days after the purchase of License for the Software. This warranty does NOT cover defects due to accident, or abuse occurring after your receipt of the Software. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

Limited Warranty on Hardware

Cabletron Systems warrants that Products delivered hereunder shall be free from defects in materials and workmanship for a period of one (1) year from the date of purchase. The liability of Cabletron Systems is limited to replacing or repairing, at Manufacturer's option, any defective Products that are returned F.O.B. Manufacturer's factory, California. In no case are Products to be returned without first obtaining permission and a customer return material authorization number from Manufacturer. THIS WARRANTY DOES NOT APPLY TO DEFECTS DUE DIRECTLY OR INDIRECTLY TO MISUSE, ABUSE, NEGLIGENCE, ACCIDENT, REPAIRS OR ALTERATIONS MADE BY THE CUSTOMER OR ANOTHER PARTY OR IF THE CABLETRON SYSTEMS SERIAL NUMBER HAS BEEN REMOVED OR DEFACED. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

EXCEPT FOR THE WARRANTY SET FORTH HEREIN, MANUFACTURER DISCLAIMS ALL WARRANTIES WITH REGARD TO THE PRODUCTS, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Hardware and Software Limitations

Cabletron Systems does not warrant that the Software will be free from error or will meet your specific requirements. You assume complete responsibility for decisions made or actions taken based on information obtained using the Software. Any statements made concerning the utility of the Software are not to be construed as unexpressed or implied warranties.

CABLETRON SYSTEMS SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS SOFTWARE LICENSE AGREEMENT, THE HARDWARE, OR THE AGREEMENTS OF WHICH THEY ARE A PART OR ANY MEDIA ATTACHMENT, PRODUCT ORDER, SCHEDULE OR TERMS OR CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: A) FOR LOSS OR INACCURACY OF DATA OR (EXCEPT FOR RETURN OF AMOUNTS PAID TO CABLETRON SYSTEMS THEREFORE), COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, B) FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING BUT NOT LIMITED TO LOSS OF REVENUES AND LOSS OF PROFITS; HOWEVER CAUSED, WHETHER FOR BREACH OF WARRANTY, BREACH OF CONTRACT, REPUDIATION OF CONTRACT, NEGLIGENCE OR OTHERWISE.

NEITHER CABLETRON SYSTEMS NOR ANY OF ITS REPRESENTATIVES, DISTRIBUTORS OR OTHER RESELLERS MAKES OR PASSES ON ANY WARRANTY OR REPRESENTATION ON BEHALF OF CABLETRON SYSTEMS' THIRD PARTY SUPPLIERS.

POST WARRANTY SERVICES

Contact Cabletron Systems for information regarding post-warranty hardware and software services.

Federal Communications Commission (FCC)

Part 15 CLASS B Statement

Section 15.105(b) of the Code of Federal Regulations

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant of Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Part 68 Statement

This equipment complies with Part 68 of the FCC rules. On the back of this equipment is a label that contains, among other information, the FCC registration number for this equipment. If requested, this information must be provided to the telephone company.

This equipment has the FCC Digital Interface Code of 02IS5. The FCC Service Order Code is 6.OY.

The USOC jack for this equipment is RJ49C.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advanced notice is not practical, the Telephone Company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities , equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advanced notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact Cabletron Systems for warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved.

No repairs can be done by the customer.

It is recommended that the customer install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightning strikes and other electrical surges.

Industry Canada

CS03 Statement

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document (s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunications Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.
User should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present,
are connected together. This precaution may be particularly important in rural areas.

CAUTION: Any changes or modifications not expressly approved by the party responsible for this device could void the user's authority to operate this equipment.

Canadian D.O.C. Notice

This product conforms with Canadian Class B emissions regulations.
Ce produit se conforme aux réglements d'émission canadienne classe B.

Instructions for Trained Service Personnel Only

CAUTION: Danger of explosion if battery is incorrectly placed. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Approvals

Safety: EN60950, UL 1950, CUL to CSA 22.2 No. 950
Emissions: FCC Part 15 Class B, EN55022/CISPR22 Class B, VCCI Class 2
Telecommunications: FCC Part 68, IC CS-03

Table of Contents

Introduction

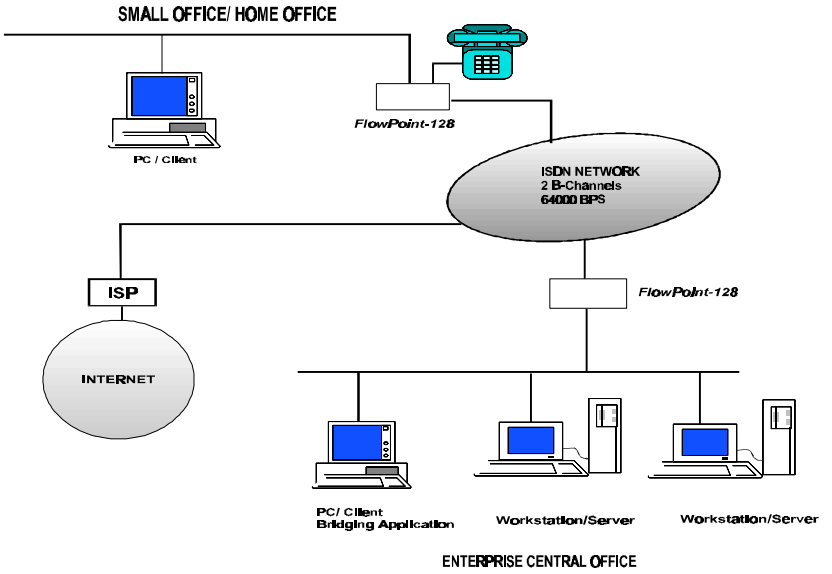
About the Router

The Cabletron Router[1] is a bridge/router designed to provide remote Ethernet LAN connectivity via a single ISDN line for the small office or home office (SOHO). The multi-protocol router offers telecommuters, home and remote office workers high-speed, dial-up access to remote sites, such as the Internet and the enterprise network. The Router supports IEEE 802.1D transparent bridging, IP routing and, optionally, IPX routing between Ethernet LAN networks across an ISDN WAN resource.

The router features an easy-to-use Windows-based management application. It can also provide two-line analog support for convenient, low-cost use of standard telephone, facsimile, modem, and answering machine equipment over the ISDN line. The router manages incoming and outgoing calls, giving analog calls priority over data traffic as needed.

The router supports Network Address Translation (a.k.a. **NAT)** which lets multiple users of a router share simultaneously one low-cost ISDN Internet connection.

Following is a sample network configuration:



[1] Throughout this manual, the Cabletron CSX100 router is called the router.

About This Book

The *User Guide* contains an introduction to the router and provides the steps and basic information needed to install and configure the router. Hardware installation and configuration of network connections, bridging, routing, and security features are described.

Note: For router hardware and software references, consult your model-specific Quick Start Guide.

Target Audience
This book is intended for small, home and remote office users, and other networking professionals who are installing and configuring the router for bridged and routed networks.

Important: If you only intend to connect to the Internet, use the Internet Quick Start guide and the Internet Quick Start Program.
If you want to connect to the Internet and use bridging or IPX, run the Internet Quick Start Program first, and then use Configuration Manager to add options.

How This Guide is Organized

This *User Guide* is intended to help you quickly install, configure, and begin using the Router. The guide is divided into eight parts:

Chapter 1, "ISDN and Ordering Issues", explains ISDN line configuration concepts and how to order your ISDN services.

Chapter 2, "Installing Router Hardware", describes how to connect the router to the configuration device, communications facilities and power source, and how to power up the router.

Chapter 3, "Installing and Accessing Configuration Manager", explains how to install and access Configuration Manager running under Microsoft Windows.

Chapter 4, "Configuring the Router with Configuration Manager", explains and lists network information that is required for configuration, and reviews the steps to configure the router using Configuration Manager.

Chapter 5, "Configuring Advanced Features", describes features used for network management and complex configuration tasks.

Chapter 6, "Management Tools", describes a set of tools used for file system management and software maintenance.

Chapter 7, "Router Feature Descriptions", lists and describes industry-standard protocols, security features, compression algorithms, network management tools.

Chapter 8, "Troubleshooting", provides suggestions for locating the source of problems depending upon the trouble symptom.

Appendices A-D provide configuration references and blank configuration tables.

A **Glossary** and an **Index** are provided at the back of this book.

References

Command Line Interface
Contains configuration and reference material for the Command Line Interface, advanced topics such as bridging and routing operations, Bandwidth-on-Demand management, PPP addressing, and a description of network management features. This manual is delivered on a DOS diskette as an Acrobat PDF document, and is supplied with the router.

Internet Quick Start Guide
Describes how to configure the router for Internet access.

Typographic Conventions

The following figure summarizes the conventions used in this guide:

Item	Type Face	Example
Words defined in glossary, book titles, figure captions	Italics	Refer to *Installing Router Hardware.*
Menu choices, keys and button names in instructions	Bold	Click **Tools**.
Examples showing you what to type	Mono-spaced font	Enter the router system name, for example: `Router1`
File names, keywords	Upper case	Copy file CFGMGR.EXE

Chapter 1. ISDN and Ordering Issues

ISDN Concepts

This chapter explains several ISDN line configuration key concepts and tells you how to order your ISDN services

Basic Rate Interface ISDN Line (U.S. only)

You will need to order one Basic Rate Interface (BRI) ISDN line from your service provider. It will provide:

- Two full-duplex 64-Kbits-per-second B-channels used for voice, data, fax, etc.
- One full duplex 16Kbps channel used for signaling.

Each B-channel can be used for a call; i.e., two calls can occur at the same time. Services vary from individual service providers.

Note: The full 64 Kbps for each channel (called clear channel) may however not be available across the entire communications link: many providers still use in-band signaling (the 8-Kbps signaling is taken from the B-channel bandwidth) so that you may only achieve a 56-Kbps channel speed.

Network Terminator

Network Terminator equipment (NT1) is required to interface between the router and the ISDN line. The NT1 offers conversion between the two-wire twisted pair (U-loop interface) used by telephone companies and the four-wire terminal equipment (S/T interface) as well as line-testing capabilities.

In North America

U Interface: The router comes with only one U interface

S/T Interface: You can order the router with an internal NT1 or use your own NT1 equipment. External Network Terminator equipment comes with a power supply (built-in or external).

In Europe and Japan

The Telephone Company provides the NT1 and offers end-users the S/T interface.

ISDN Wires

The ISDN wires are the same wires that exist for analog telephone service in most cases.

EIA/TIA standard for wiring:

- Unshielded twisted pair (UTP) cable, category 3 or above, 24 gauge
- 8-position RJ45 jacks for new ISDN service installation are recommended

Configurations

ISDN BRI lines can be configured in point-to-point and multi-point configurations and can support dual-POTS interfaces.

Point-to-point:

Only one device is connected to the ISDN line.

Multi-point:

This configuration can have up to 8 devices (ISDN telephones, ISDN terminal adapters, ISDN routers, etc.) dropped on the ISDN line.

POTS interface device support:

Up to four devices per port but only one call initiated at a time (though another call can be in progress).

Since the ISDN BRI line will be used for a high-speed LAN-to-LAN link, you need to be sure that additional devices dropped on the S/T interface of the router allow sufficient access for the router's bandwidth requirements.

SPIDs and Directory Numbers

The Network Service Provider will give you the following information for identifying the ISDN line and devices. In some countries, some of these number/addresses are not implemented and will not be provided.

Directory Numbers (DNs)

Phone numbers are assigned by the ISDN service provider for each device operating on the line. In most cases, one DN is assigned for each B-channel. Up to eight DNs can be assigned to provide numbers for additional devices on the ISDN line (see Multi-Point).

Service Profile Identifications (SPIDs)

North America: SPIDs are assigned by the ISDN service provider and identify the services and features that the switch provides to the ISDN device. The SPID is often derived from the directory number, concatenated with other digits.

Outside North America: SPIDs are not required outside of North America.

Telephone Switch Parameters

The following table contains the recommended provisioning for the three switches available in North America.
When ordering your ISDN service, some of the following information (depending on your switch) will be needed.

Provisioning Information	AT&T 5ESS w/custom software	National ISDN (NI-1)	DMS-100
B1 channel	circuit switched data & voice	circuit switched data & voice	circuit switched data & voice
B2 channel	circuit switched data & voice	circuit switched data & voice	circuit switched data & voice
D channel	signaling only	signaling only	signaling only
Multipoint	yes	yes	n/a
Terminal type	A	A	n/a
Display	off	off	n/a
Terminal endpoint identifier (TEI)	dynamic	dynamic	dynamic
Call appearances	2	2	-
Call preference	idle	idle	-
Additl. Call offerings	yes	yes	yes
Nail up	none	none	none
Ringing indicator	-	-	yes
Release key	-	-	yes

We recommend that you supply these parameters to your telephone company in the form of an IOC. It will make ordering your ISDN services a lot easier (See below, *How to order your ISDN line).*

Note: NI-1 is a standard released by Bellcore outlining a basic set of ISDN services and is switch-type independent. It is recommended as the preferred switch type.

The new EZ-ISDN 1 provisioning is also supported and is recommended.

How to Order your ISDN Line

1. Call your local telephone company's ISDN Ordering Center.

Consult with your service provider 2 weeks before requiring the installation and use of the ISDN service.

2. Specify your ISDN Basic Rate Interface line (BRI) provisioning (North America only).

To simplify your ISDN line ordering process, use one of these standard ISDN Ordering Codes (IOCs), or use the table above.
Select the package that best meets your needs.

Generic Package M includes:

- Voice and data capability on both B-channels. The D-channel is used for signaling only.

Generic Package S (most common**)** includes:

- Voice and data capability on both B-channels. The D-channel is used for signaling only.
- Calling Line ID (CLID) a.k.a Automatic Number Identification.

EZ-ISDN 1 (also know as Capability U and recommended) includes:

- Voice and data capability on both B-channels. The D-channel is used for signaling only.
- Calling Line ID (CLID) a.k.a Automatic Number Identification.
- Additional voice features

Note: The router supports this package, but voice features are only useful on models with POTS support.
Important: Point-to-Multipoint service is preferred over Point-to-Point service since you get 2 DNs. Generic Package S is best suited for Point-to-Multipoint service.

3. Request National ISDN-1 switch as your preferred switch type. (This is not required but recommended.)

4. The following information will be provided by your telephone company:

Europe: Switch type and Directory Numbers (DNs)

North America: Switch type, Service Profile ID Numbers (SPIDs), and Directory Numbers (DNs)

Asia: Switch type and Directory Numbers (DNs)

Your switch Type will be one of the following and may or may not have SPIDs associated with it:

	SWITCH TYPES	DNs	SPIDs
EUROPE	**NET3** European ISDN/ETSI	yes	no
	NET3SW Swiss NET3 variant	yes	no
NORTH AMERICA	**NI1** National ISDN-1-compliant switches	yes	yes
	AT&T 5ESS AT&T 5ESS Custom	yes	yes
	DMS100 Northern Telecom DMS-100	yes	yes
ASIA	**NTT** Nippon Telegraph and Telephone	yes	no
	KDD Kokusai Denshin Denwa., Ltd.	yes	no
	HSD64 64Kb permanent connection	no	no
	HSD128 128Kb permanent connection	no	no

Note: Save this information; you will need it later to configure your router.

5. Order long distance ISDN service (North America).

Contact the long distance company of your choice to obtain ISDN service outside of your local telephone company's service area. Here are some long distance companies and their telephone numbers for North America:

AT&T: 1-800-222-7956

MCI: 1-800-MCI-ISDN

Sprint: 1-800-736-1130

When ordering your long distance ISDN service, specify:

- ISDN Circuit Switched Data capability (clear channel 64 Kb)
- Voice for both B-channels

Chapter 2. Installing Router Hardware

Before You Begin…

Router Package Contents

You should find the following items in your router package:

- Router
- Twisted pair Ethernet (TPE) crossover cable (yellow label marked "**Ethernet 10 Base-T, Crossover**")
- WAN and ISDN attachment cable (blue label marked "**ISDN or ADSL**")
- Console cable with adapter (green label marked "**Console**")
- Power cable
- Diskettes containing Configuration Manager and the *Command Line Interface* manual
- *User Guide* (this manual)
- *Internet Quick Start* guide

Package Contents Inspection

Be sure to inspect the equipment contained in this package prior to installation to ensure that the router has not been damaged during shipment. You should report any damage to the freight carrier. **DO NOT ATTEMPT TO INSTALL OR OPERATE DAMAGED EQUIPMENT.**

Model Features and Numbers

Important: For router hardware reference, consult the model-specific Quick Start Guide.

The router contains:

- One Ethernet port
- One RS232 asynchronous console port

- One ISDN Basic Rate Interface (BRI) port (with built-in U interface)
- Models 104, 105, and 107 support 2 analog device ports for POTS (Plain Old Telephone Service)
- Built-in power supply

Series Number	Model Number	ISDN Interface	2-Line POTS	LAN Devices Supported
International	101	S/T	No	Unrestricted
	104	S/T	Yes	Unrestricted
North America	103	U	No	Unrestricted
	105 and 107	U	Yes	Unrestricted

Hardware Installation

Telephone Wiring Cautions

If you must install or alter existing telephone wiring, be sure to take the following precautions:

- Do not install telephone wiring during a lightning storm
- Do not install telephone jacks in wet locations.
- Do not touch non-insulated telephone wires.

Installation Overview

Select a suitable location for installing the router. The router can be placed on a table or other horizontal surface. Provide sufficient space at the rear of the unit (a few inches) for proper air circulation. Before installation, ensure the unit is powered off.

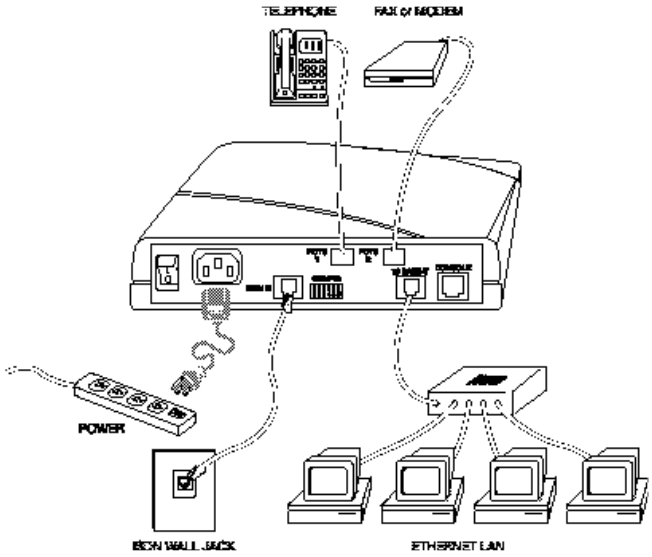
To install router hardware, you will perform the following operations:

1. Connect the router to the Ethernet LAN
2. Connect the router to an ISDN line
3. Connect phone, fax, or analog modem device to POTS interfaces
4. Connect the router to an AC power source

Note 1: Non-Windows users will have to additionally connect the router console port to their computers to be able to initialize the router's IP address and configure the router. Refer to Appendix D, *Access the Command Line Interface (CLI)* for more details.

Note 2: The Console interface is not used.

The following diagram shows the back panel the CSX105 router and the location of jacks for connecting the ISDN equipment, analog device equipment, and the Ethernet hub.

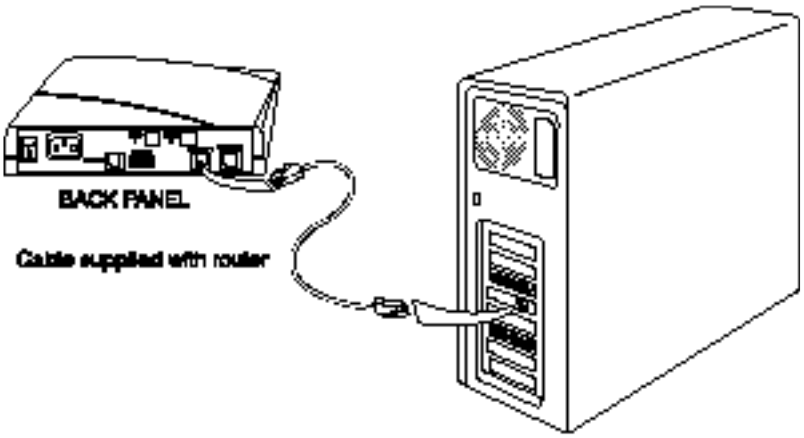


Step 1. Connect the Router to the Ethernet LAN

The 10Base-T port is used for Ethernet communications for single station or hub configurations. Connect the Ethernet LAN using the following instructions.

Configuration A: Ethernet single station

Single Station

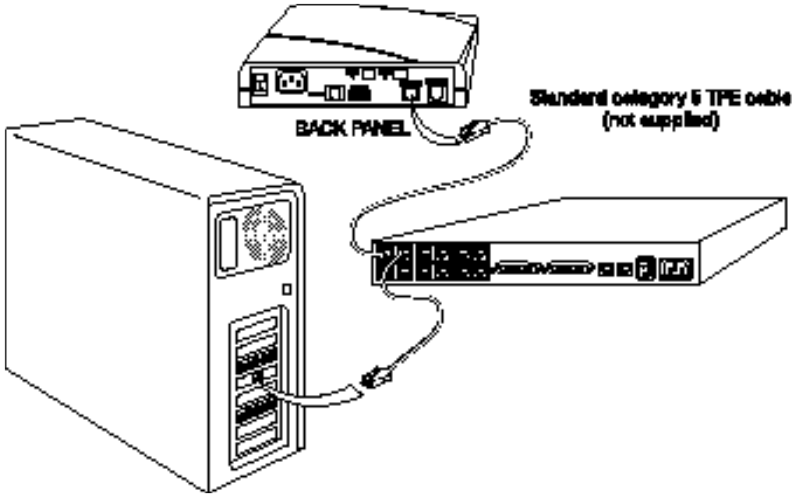


Instructions:

1. Connect the 10Base-T Ethernet cable (yellow label marked "**Ethernet 10 Base-T, Crossover**") to the RJ45 twisted pair Ethernet (TPE) jack marked **10 Base-T** on the unit.
2. Connect the other end to the Ethernet board in your PC.

Configuration B: Ethernet hub

Hub Attachment

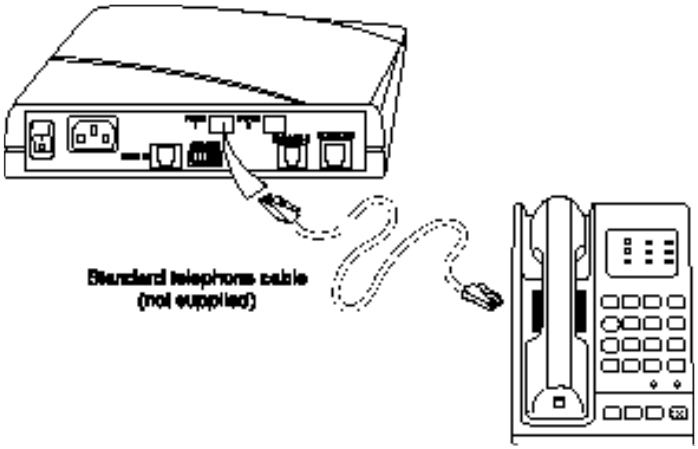


Instructions:

1. Connect the 10 Base-T Ethernet cable (a standard category 5 TPE cable, **NOT SUPPLIED**) to the RJ45 twisted pair Ethernet (TPE) jack marked **10 Base-T** on the unit.
2. Connect the other end to the Ethernet board in your PC.

Step 2. Connect Analog Telephone Devices

If you are installing model CSX104 or CSX105, your router will have two POTS interfaces on the rear of the unit.



Instruction:

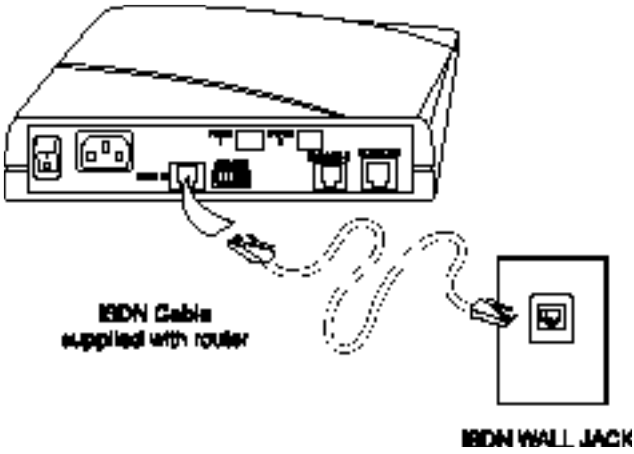
Connect one or more phone, fax, answering machine, or other local analog equipment to the **POTS** jacks on the back panel. You can attach multiple devices to one **POTS** jack using a splitter connector.

Step 3. Connect the Router to an ISDN Line

In North America, ISDN U interface models

These models were designed specifically for North America, where a network terminator interface (NT1) is needed. This NT1 is built into the router and is “transparent” to the user.
These models have only one **ISDN U** jack on the rear of the router.

U.S. Configuration: U Interface



Instructions

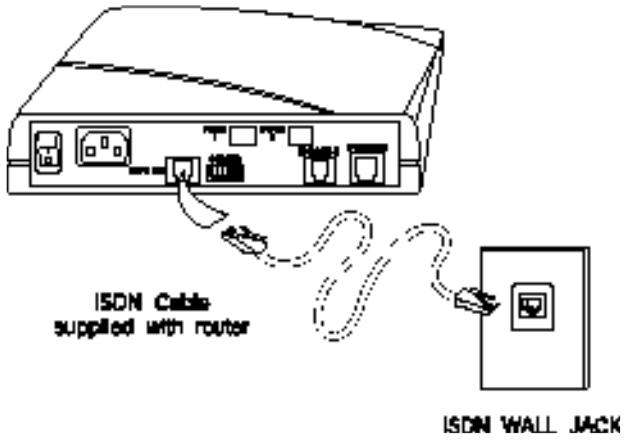
1. Plug one end of the ISDN cable (blue label marked “**ISDN or ADSL**”)
   into the RJ45 jack marked **ISDN U** on the back panel of the router.
2. Plug the other end of the cable into the RJ45 ISDN wall jack.

Outside North America, ISDN S/T interface models:

These models were designed for international (outside North America) markets where the NT1 is typically provided by the ISDN service provider. These models have one **ISDN S/T** jack on the rear of the router where the ISDN line is plugged in.

Note: Refer to Chapter 1 for more details on ordering and configuring an ISDN line.

International (outside North America) Configuration: S/T Interface



Instructions

1. Plug one end of the ISDN cable (blue label marked "**ISDN or ADSL**") into the RJ45 jack marked **ISDN S/T** on the back panel of the router.
2. Plug the other end of the cable into the S/T bus RJ45 **ISDN** wall jack.

   Note 1: You may connect multiple devices on the same wire in a multi-point bus configuration with a splitter. If the router is in a multi-point bus configuration and it is not on either end of the bus, switches controlling termination must be set to off (See Appendix A).

   Note 2: Routers outside North America do not have an ISDN U interface connector.

Step 4. Connect the Router to an AC Power Source

The router comes with a built-in power supply and a standard power cable.

Instructions

1. Check to see that the power switch (**0=off, 1=on**) on the rear of the router is set **off**.
2. Connect the power cable (packaged with the router) to the AC power connector on the back panel of the router and plug the other end into an AC outlet.
3. After connecting the power source, turn the switch **on**. The router will execute a Power-On-Self-Test (POST) when the unit is powered on. During this test, channel lights will flicker. After successful completion of the POST and boot of router software, the lights will reflect ready status. Check the front panel of the router and you should see that:

In North America:

- **PWR** light is lit green.
- **LINE** light is blinking or solid if the correct DNs and SPIDs are found and accepted.
- **NT-1** light is on indicating physical connectivity on the ISDN line. If the lights do not reflect the **ready** state as indicated above, refer to the section *Troubleshooting*.

Outside North America:

- **PWR** light is lit green.

Chapter 3. Installing and Accessing Configuration Manager

This chapter describes how to install and access **Configuration Manager** running under Microsoft Windows.

About Configuration Manager

Configuration Manager is an easy-to-use, point-and-click graphical user interface (GUI), thus making it the ideal tool to perform all the configurations described in this guide. It is a Windows-based application and can run under Windows for Workgroups, Windows 95, and Windows NT**.**

Configuration Manager allows you to configure the router's system settings, routing and bridging function, remote router access, bandwidth management, and security features.

It also includes a set of tools designed to simplify some configuration tasks. Personal computer hardware and software prerequisites needed to run Configuration Manager are listed in the following section.

An Ethernet LAN connection between the router and the personal computer is needed to configure the router using the Graphical User Interface.

Note: If you only intend to connect to the Internet, please use the Internet Quick Start guide and application instead.

Important Note:

There are a few "unusual" situations where users have to use the **Command Line Interface** instead of **Configuration Manager** to configure the router, as listed below:

- IP address initialization and router configuration for **non**-Windows-based platforms (such as Macintosh and UNIX)
- Advanced settings of DHCP, filters, or ISDN Dial-Back for example
- Changing an existing IP address

The Command Line Interface requires a console or Telnet connection. Detailed information about installing and accessing the CLI is described in Appendix D, *Accessing the Command Line Interface (CLI).*

Hardware and Software Prerequisites

Configuration Manager requires the following hardware and system configuration:

- IBM-compatible Personal Computer
- Ethernet network interface card
- 8.0 MB of hard disk space (5.0 MB for Configuration Manager and on-line documentation plus up to 3.0 MB for the files to be installed in the \WINDOWS\SYSTEM directory)
- Microsoft Windows 3.1, Windows for Workgroups, Windows 95, or Windows NT
- Winsock 1.1-compliant TCP/IP stack installed and running on your PC (included with Windows 95)

Install Configuration Manager

To access Configuration Manager, you will first configure your PC to obtain an IP address automatically, and then install the Configuration Manager application.

Note 1: Windows 95 is assumed throughout this section.

Set your PC to obtain an IP address

This section assumes that you have already:

- connected the router's cables.
- powered on the router.

Instructions

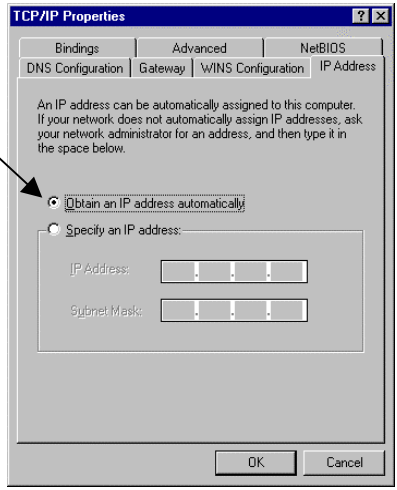
1. From the taskbar, click the **Start** button, select **Settings, ➢ Control Panel**, ➢ **Network**.
2. You are now in the **Network** window. In the **Configuration** tab page, double-click **TCP/IP** (to configure your network adapter).

3. In the **TCP/IP Properties** window, in the **IP Address** tab page, enable **Obtain an IP address automatically** by clicking the button next to it.

4. Click **OK**.

5. Answer **Yes** to "Do you want to restart your computer?" Your computer will reboot.

(**Note:** If your settings were already configured with these attributes, you will not be prompted to reboot and a reboot is not necessary.)



Install Configuration Manager on your PC

This section assumes that you have already:

- connected the router's cables.
- powered the router on.
- set your PC to obtain an IP address.
- rebooted your PC.

Instructions

The three diskettes included in the router box contain Configuration Manager, the Internet Quick Start program (a configuration utility for Internet users) and an electronic copy of the *Command Line Interface* manual.

1. To install the Configuration Manager program, insert diskette #1 in drive A: (or B:) of your PC.

2. Select the **Start** button. In the dialog box provided under the **Run** menu item type:

   `A:\SETUP.EXE` (or `B:\SETUP.EXE`)

Configuration Manager will be installed in the C:\CFGMGR directory by default. You may however choose to install it in another directory.

Access Configuration Manager

1. Click the **Start** button on your PC desktop.
2. Select **Programs.**
3. Select **Cabletron Configuration Manager.**
4. Click the **Configuration Manager** icon.

The following screen is the Configuration Manager's main menu, before you connect to the router:

Chapter 4. Router Configuration

Planning for Router Configuration

This section describes configuration terminology and the information that you need to collect before configuring the router.

Important Terminology

You should familiarize yourself with the following terminology, as it will be used throughout the configuration process. The diagram illustrates these key words/concepts.

Target router: Router that you are configuring. Also referred to as **local** router.

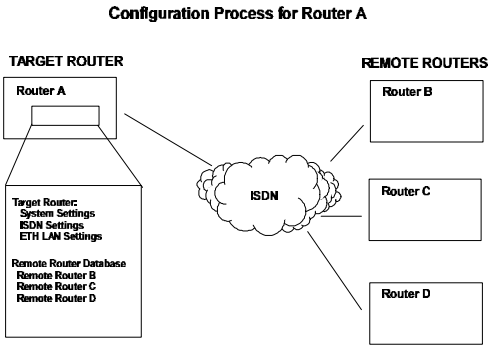
Remote routers: All the routers to which the target (local) router may connect.

Remote router database: Database which resides in the target router and contains information about the remote routers to which the target router may connect.

Remote router entry: Entry about a remote router in the target router database. A remote router entry defines:

- Connection parameters
- Security features
- Route addressing and bridging functions

The following diagram illustrates these key words and concepts.



Important Routing Concepts

TCP/IP Routing

The purpose of IP routing is to take the IP destination address and look up the interface on which the packet should be forwarded. In the case of the router, this can be either the LAN (Ethernet) or the WAN. Because each remote entry has an IP route associated with it, this may involve first bringing up the link to that destination in order to allow forwarding to take place.

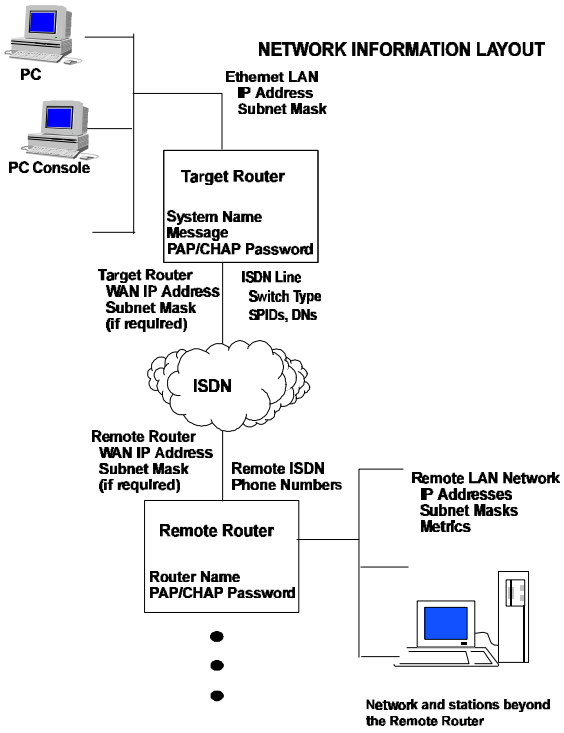
Ethernet interface
Each Ethernet interface needs to have defined an IP address and subnet mask.

ISDN WAN interface
The IP address and mask can be defined statically (Static Seeding),
- or -
The IP address and mask can be assigned dynamically through the PPP Protocol,
- or -
An IP address and mask may simply not be required (Unnumbered mode).

The exact detail for how the WAN port needs to be configured depends upon the requirements of the router at the remote end. Normally, the required information is passed between the routers using the PPP Protocol, thus no manual configuration is required.

When the local WAN interface has an IP address and mask defined, the remote WAN interface also has an IP address and mask associated with it. These interfaces are known as the **local (source) WAN IP address** and the **remote WAN IP address.**

Each remote router ISDN WAN link may have local and remote WAN IP addresses and subnet masks depending on the method of IP addressing used. The IP routing table in the target router can be ‘seeded’ with addressing information for networks/stations beyond the remote router.



TCP/IP Route Addresses

Static Seeding: If the router is to direct traffic to networks or stations beyond the remote router, the routing table in the target router can be 'seeded' with static IP routes. An IP route includes an IP address, subnet mask, and metric. The metric is a number representing the perceived cost in reaching the remote network or station.

The target router's routing table must be seeded statically so that it dials out to the appropriate remote router when IP traffic is addressed to networks and stations beyond that remote router. After the link is established, RIP update packets will dynamically add to the target router's routing table.

Note: Seeding the routing table is not necessary when a target router never dials out; it will discover remote networks and stations beyond the calling router as soon as RIP updates arrive (provided the remote router supports RIP and RIP packets are allowed to flow on the WAN link).

TCP/IP Default Route

One default route should be designated in the routing table for all traffic that cannot be directed to other specific routes. The default route is specified as: **0.0.0.0 255.255.255.255 1**

You will need to define the default route for a remote router (if the target router will be placing calls to that remote router). There can be only one default route specified for all the remote database entries.

Note: You cannot have more than one router configured to advertise itself as the default router. Usually, this not a problem since most organizations have only one router. However, if you have more than one router, be sure to choose only one router as the default router and change the configuration of the other routers accordingly.

Source (Target) and Remote WAN IP Addresses

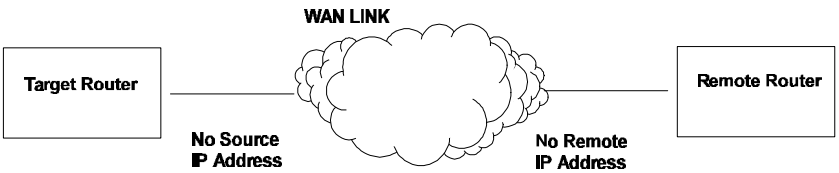
You may need to specify a source WAN IP address and/or a remote WAN IP address for the WAN connection to the remote router depending on IP address negotiation under PPP. Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required. The three possible scenarios are illustrated on the next page.

In unnumbered mode, neither IP address is defined on the WAN link. In numbered mode, one IP address is defined on each end of the WAN link. These addresses may or may not belong to the same subnetwork. They may also be determined automatically, negotiated, or forced by the network administrator.

The Router runs in unnumbered mode or numbered mode, determined automatically. If unnumbered mode negotiation fails, numbered mode is attempted using the Ethernet LAN IP address as a default source WAN IP address. If you have specified a source WAN IP Address, unnumbered mode negotiation is not performed; i.e., the operating mode is numbered. If a source WAN IP address is explicitly defined, the router will not, as a rule, accept another local address from the remote end. In numbered mode without an explicit Source WAN IP address, this address can be negotiated to a different value by the remote end.

If the remote router supports unnumbered mode, neither address needs to be specified.

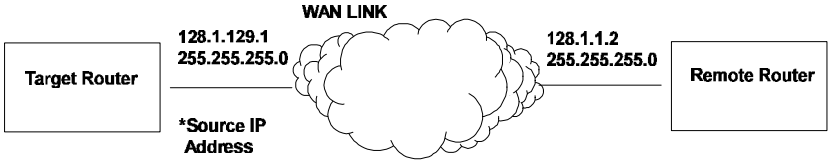
Unnumbered Mode



For numbered mode, consider the capabilities of the remote router as well as your requirements. Specify a Source WAN IP Address if the target

router must be on the same subnetwork as the remote router. The following illustration is an example of a subnet (128.1.129.0) of Class B IP network (128.1).

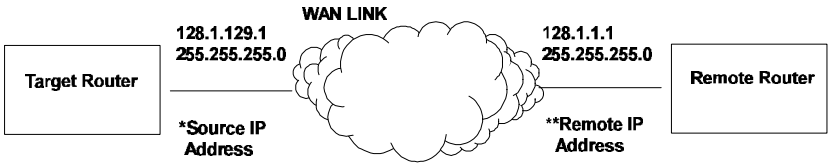
Numbered Mode
Same Subnetwork as Remote



*Specify source IP address if it must be on the same subnetwork as the remote router.

Specify a Remote WAN IP Address if the remote router does not support IP address negotiation under PPP (i.e., does not have a pre-assigned IP address).

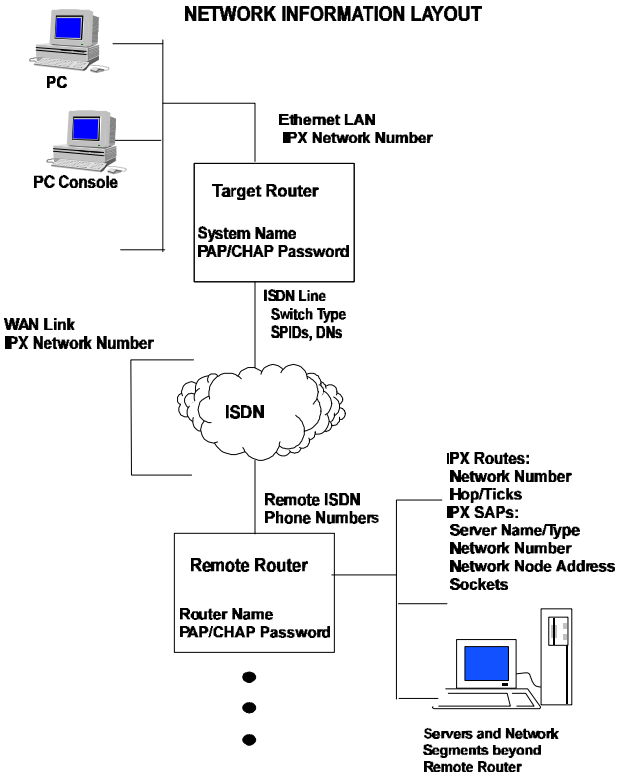
Numbered Mode
Remote Router w/o pre-assigned IP address



*If source IP address not defined, defaults to Ethernet LAN IP address
**Specify remote IP address if remote router does not have a pre-assigned IP address.

IPX Routing

An Ethernet LAN IPX network number is required for the router's local Ethernet LAN connection. The ISDN WAN link to each remote router must have an assigned IPX network number. IPX Routes and IPX SAPs for each remote router are also required for the configuration process.



IPX Routes

If the router is to direct traffic to network segments and servers beyond the remote router, the routing table in the target router can be 'seeded' with static IPX routes. An IPX route includes:

- a network number
- a hop count (the hop count is the number of routers through which traffic must pass to reach the remote network segment or server)
- a number of ticks (the number of ticks represents how much time the packet takes to reach the destination in units of roughly 1/20th of a second)

The target router's routing information table must be seeded statically so that the target router dials out to the appropriate remote router when IPX traffic is targeted to network segments or servers beyond that remote router. After the link is established, RIP update packets will dynamically add to the target router's routing information table. Seeding the routing table is not necessary when a target router never dials out; it will discover routes beyond the calling router as soon as RIP updates arrive (provided the remote router supports RIP). However, for watchdog spoofing to work, the remote IPX Routes for network segments and servers should be defined.

IPX SAPs

If the router is to obtain services beyond the remote router, the target router's SAP services table must be seeded statically. A SAP service is identified by:

- a server name and corresponding server type
- network number
- node number
- socket (the socket number represents the service (application) within the server node

The target router's SAP services table must be seeded statically so that the target router can direct traffic to the appropriate remote router when a service is requested from a server beyond that remote router. After the link is established, SAP broadcast packets will dynamically add to the target router's services table. Seeding the table is not necessary when a target router never dials out; it will discover remote services beyond the calling router as soon as SAP broadcasts arrive (provided the remote router supports IPX).

IPX Network Numbers

IPX network numbers are assigned to LAN network segments as well as servers. These numbers should be unique for all IPX networks on the Internetwork.

IPX external network numbers refer to the physical LAN network segments to which servers and routers are connected. The WAN link network number is an external IPX network number. This is a unique number that you choose (or are given by the network administrator) to represent the WAN link between the target router and remote router. The local Ethernet IPX network number is also an external network number.

Servers are identified with internal network numbers. This is a logical network number that identifies the individual server. For a local router to access a server beyond the remote router, you will specify a route using the internal network number of a server. To seed the routing table to access a network segment, you will specify the external network number of the LAN segment. The network number in the SAP table is the internal network number of the server.

Node Numbers

Servers can have internal and external node numbers. The internal node number is a logical number assigned by the system administrator to the server. The external node number is the MAC address of the NIC in the server. When adding SAP services to the SAP table, internal node numbers are used.

Collect Your Network Information

You should obtain, define, and specify information about the target router's network before you start configuring your router. This simple step will save you time and make the configuration process a lot easier. Use the Network Information Worksheets in Appendix C to collect your network information.

For the Target router, you need to define and obtain:

- Its own name and security password (defined by the user)
- ISDN line information (obtained from the ISDN service provider)
- The Ethernet LAN IP and/or IPX address (defined/specified by the user or provided by the network administrator)

In the Target's remote database, you need to identify:

- The remote router(s)
- Their routing and bridging capability
- ISDN phone numbers
- Addressing and security information

If you are using IP routing, you also need to decide if you will use Internet Firewall filtering.

Names and Passwords

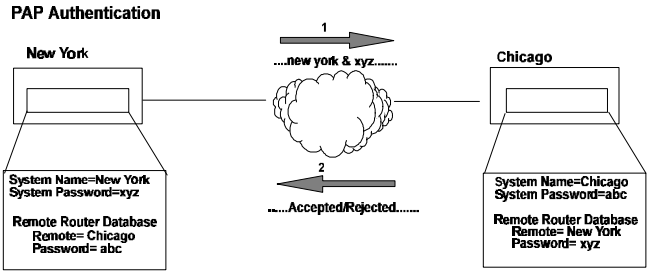
Name and Password for the Target router

You must choose a name and authentication password for the target router. They are used by a remote site to authenticate the target router.

Names and Passwords for the Remote Router(s)

For each remote router, you must have the router name and its authentication password. They are used by this target router to authenticate the remote router. The name and password are used in both PAP and CHAP authentication. The following diagram shows how this information is used.

Note: A useful *Names and Passwords Example* is provided, page 66.



ISDN Line Information

The following information should be obtained from your ISDN service provider:

ISDN switch type

The switch types supported are listed in chapter 1, page 7.

Directory Numbers (DNs) or Phone Numbers

Phone numbers assigned by the ISDN service provider for each device operating on the line. Used for others to dial into the ISDN B-channels on your ISDN line. This number can be similar to the phone number.

Note: The Directory Number is generally not implemented outside North America.

Service Profile Identifications (SPIDs)

SPIDs identify the services and features that the switch provides to the ISDN device. Commonly implemented in the U.S. and Canada, the SPID is often derived from the directory number, concatenated with other digits.

Note: SPIDs are not implemented outside North America.

Refer to Chapter 1, *ISDN and Ordering Issues*, for further information.

TCP/IP Routing Entries

You will need to obtain the following network addresses:

For the Ethernet Interface

Ethernet IP Address (Local LAN)
An Ethernet LAN IP address and subnet mask are required for the router's local Ethernet LAN connection.

TCP/IP Ethernet Routes
You normally do not need to define an Ethernet IP route. An Ethernet IP route consists of an IP address, a mask, a metric, and a gateway. An Ethernet route is usually defined when there are multiple routers on the Ethernet, which cannot exchange routing information between them.

Ethernet Default Gateway
One default route should be designated in the routing table for all traffic that cannot be directed to other specific routes.
You will need to define the default route to a remote router or define an Ethernet gateway. There can be only one default route specified for all the remote database entries.

For the ISDN WAN Interface

Source (Target/Local) WAN Port Address
You may need to specify a source WAN IP address for the WAN connection to the remote router depending on IP address negotiation under PPP.
Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required. The router is set to unnumbered mode by default. This enables numbered mode on the WAN interface.

Remote WAN Address
You may need to specify a remote WAN IP address for the WAN connection to the remote router depending on IP address negotiation under PPP.
Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required. The router is set to unnumbered mode by default. This enables numbered mode on the WAN interface.

TCP/IP Remote Routes
An IP route includes an IP address, subnet mask, and metric (a number representing the perceived cost in reaching the remote network or station).

- **TCP/IP Default Route**
  A default route should be designated in the routing table for all traffic that cannot be directed to other specific routes.
  You will need to define the default route to a remote router or, if required due to special circumstances, define an Ethernet gateway.
  There can be only one default route specified for all the remote database entries.

Advice: It is often helpful to draw a diagram including all locations, addresses, router names, etc. The following diagram shows the information required to configure ***only*** the target router's side. If you need to configure both ends of the WAN link, you will want to label all information for the network.

IPX Routing

If you are configuring IPX routing, you will need to obtain the following information (most likely from your network administrator).

Note: IPX routes define a path to a specific destination. They are primarily needed by the routers to allow the servers and clients to exchange packets. A path to a file server will be based on the Internal Network Number of the server.

A path to a client will be based on the External Network Number (Ethernet) of the client.

Internal Network Number

It is a logical network number that identifies an individual Novell server. It is needed to specify a route to the services (i.e. file services, print services) that Novell offers. It must be a unique number.

External Network (a.k.a. IPX Network Number)

It refers to a physical LAN/wire network segment to which servers, routers, and PCs are connected (Ethernet cable-to-router segment). It must be a unique number. Number

WAN Network Number

Important: This number is not part of the routing information. This number identifies the WAN segment between the two routers only. Note that only one router needs to have the WAN Network Number configured. The other router will learn it.

SAP (Service Advertisement Protocol)

SAP entries should reflect primary logon servers for the clients on the local LAN. Only the servers on the remote side of the link have to be entered. Local servers do not need to be entered.

Frame type

With local servers on your LAN, make sure to select the proper frame type for the IPX network number. To determine this, consult with your network administrator. When you have only NetWare clients on your LAN, leave the default (802.2) selected as most clients support any type. The frame type choices are:

802.2 Default recommended by Novell

802.3 Other most common type

DIX For DEC, Intel, Xerox; this setting is also referred to as “Ethernet II”, and is rapidly becoming obsolete.

Configuration Steps

Overview

If you have collected the required information as described in the preceding section, you are ready to configure the router.

Using Configuration Manager, you will perform the following basic configuration steps:

1. **Connect, Select the Router to configure, and log into the target router.**

2. **System Settings**

   Configure the target router's system settings including:

   - System Name
   - System Message (optional)
   - Dial Authentication Password
   - Ethernet IP Address and LAN RIP Settings
   - DHCP Settings
   - If configuring IPX: Ethernet IPX Network #
   - Change Login Password (optional)

3. **ISDN Settings**

   Configure the target router's ISDN Settings including:

   - ISDN Switch Settings: SPIDs, DNs, Switch type
   - Analog Phone Settings (for POTS routers)

4. **Remote Routers**

   Add Remote Routers to the remote router database and configure the following remote router information:

   - ISDN Dial Settings: Caller ID, Call Back information, Bandwidth management controls
   - Security information
   - Bridging capability

- TCP/IP route addressing and routing protocol controls
- If configuring IPX: IPX Routes addressing and IPX SAPs services

5. **Bridging / Routing**
   - Set the default bridging destination
   - Enable IP routing
   - If configuring IPX: Enable IPX routing
   - Enable the Internet Firewall
   - Enable WAN-to-WAN Forwarding

6. **Store**

   Save the router's configuration

7. **Reboot the router**

8. **Verify the router's configuration**

As you step through the configuration, each setting you change results in a dynamic update of the router's configuration. Some changes, though, don't take effect until you store the configuration and reboot the router.

Note: Changes requiring a reboot of the router

System Settings:
Ethernet IP
IPX Address and options

Bridging and Routing Controls:
TCP/IP Routing
IPX Routing
Default Bridge Destination

Remote Router:
TCP/IP Route Addresses
IPX Routes
IPX SAPs
Bridging
Add or remove remote router entries

Step 1. Connect and log into the Target Router

This section assumes that you have already installed Configuration Manager on your PC and know how to access it (otherwise, refer to Chapter 3, for details).

Connect

The router is shipped to users with a default IP address that does **not** need to be changed (however, to change the default IP address, refer to Step 2. *Ethernet LAN Address and Protocol*). This default address is 192.168.254.254.

⇒ Click the **Connect** button to connect your PC to the target router. This will open the **Select the Router** window where the default IP address (192.168.254.254) is already entered.

⇒ Click **OK**.

If Configuration Manager cannot connect successfully to the target router, you will get a message asking you if you wish to retry to connect.

If you cannot connect to the router:

Verify the router's LAN IP address and subnet mask by using the Terminal Window (under **Tools**) and typing **`eth list.`**

Check the PC and router's physical connections to the LAN.

First-time Connection Messages

The first time that you connect to the router, a message will inform you that the firmware file is being automatically backed up from the router to the PC.

If you have been supplied with an **Installation Script**, you may, with your initial connection to the router, execute it. Follow the instructions on screen. Otherwise, click **No**.

Password, Login, Skip

⇒ Enter the Login Password **`"admin"`** in the **Login** window.

This security feature allows you to prevent unauthorized write access to the router's configuration. The default login password is **`"admin"`** when first configuring the router. Type it in lowercase and verify that your keyboard Caps Lock key is not active. After successfully connecting to the router, the main menu screen will appear.

Note: If you only want to view the router's configuration settings:

⇒ Click **Skip.**

If you attempt to change any of the router's configuration settings while in **View-Only mode**, you will again be prompted for the write enable **Login Password**.

Name, Message, Software, Hardware, About

Name is the name for the target router.

Message is an informational message that you can enter and save for this target router display.

The **Name** and **Message** fields are blank for the initial configuration. If you click either of these fields after the label, a menu is displayed allowing you to alter this information. You do not need to do this at this time; this is the same menu displayed when you click the button **System Settings** later in the configuration process.

Software is the target router's software level.

Hardware is the Model Number, Serial Number and Revision Level of the router.

The **About** button is used to display Configuration Manager's version number, date, and SNMP DLL version.

If you need to supply Technical Support with a technical information log file, press the **Tech Info** button to collect the information.

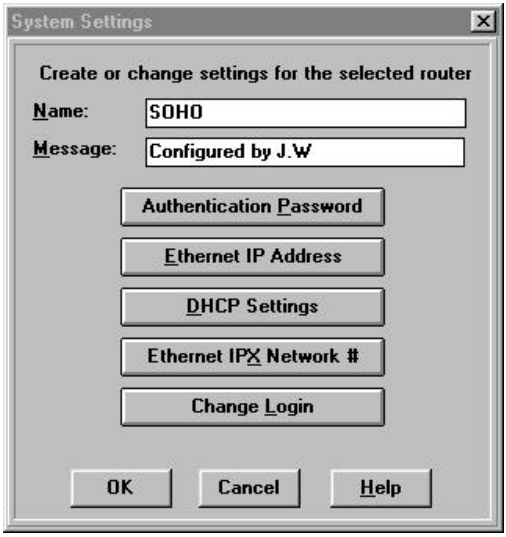
Step 2. Target Router's System Settings

You will now enter information about the target router you are configuring and adding to your network. This information includes:

- The system name
- An optional system message
- A dial authentication password
- Ethernet IP address
- DHCP

- Ethernet IPX address (if you are configuring IPX)
- Change the login password (optional)

⇒ Click **System Settings** from the main menu. The **Name** and **Message** fields are blank when you first configure the router.



System Name

⇒ Enter a router name in the field labeled **Name**.

You **must** enter a system name for the target router. This name is sent to other routers during dial-up authentication. Space characters within the name are converted to underscores, as the system name is a 'word' when exchanged with PAP/CHAP.

System Message

⇒ You may enter an optional system message in the field labeled **Message**.

This message is saved in the router and is displayed on Configuration Manager's main menu screen. This field is useful for specifying, for example, the name of the person configuring this router and the last changes made.

Authentication Password

The target router's dial authentication password is used for authentication when the target router dials out to other routers or is challenged by them. The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one.

⇒ To set the password, click **Authentication Password** and enter the new password twice in the small window.

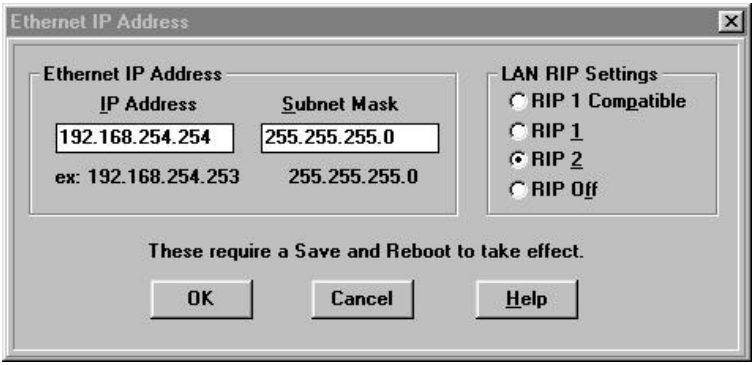
⇒ Click **OK** to set the password.

Ethernet IP Address and LAN RIP Settings

You have the option to enter or change your router's Ethernet IP address and IP protocol control information (LAN RIP Settings).

Ethernet IP Address

For IP routing, click **Ethernet IP Address** if you wish to change the Ethernet IP address and subnet mask from the default. The following window displays the default IP address and subnet mask (factory default).



Changing the IP Address and Mask

⇒ Use this window if you wish to change the router's IP address and subnet mask. This may occur, for example, if a company already has a LAN network and users are given specific addresses to use by their network administrator.

⇒ Click **OK** to save the changes and exit the window.

Note: If you change either of these fields, you must always perform a **Store** and **Reboot** as shown in later steps.

LAN RIP Settings

To change the default RIP settings, refer to *Routing Information Protocol*, page 73.

DHCP

The router supports **DHCP**, and acts as a DHCP server. This allows hosts (PCs, etc.) to acquire initialization parameters (IP addresses, masks, domain names, etc.) from the router. DHCP is enabled by default.
For more information on DHCP configuration, refer to Chapter 5. *Configuring Advanced Features.*

Ethernet IPX Network Numbers

If you are configuring the router for IPX routing, click **Ethernet IPX Network #**.

⇒ Enter your IPX Network Number. Select the appropriate frame type.

⇒ Click **OK** to save the changes and exit the window.

The IPX Network Number (also known as the External Network Number) is an 8-character hexadecimal string representing the Ethernet LAN. You can now use this window to change the settings.

The frame types must be compatible with the Novell server located on the same LAN. To determine this, consult with your network administrator.

Note: you must always perform a **Store** and **Reboot**, when entering or changing information in this window.

Change Login Password

⇒ If you wish to change the login password from the default (`admin`), click **Change Login** on the main menu.

⇒ In the **Login Password** window, enter a new password in the fields provided.

The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one set.

⇒ Click **OK** to set the password.

Step 3. Target Router's ISDN Settings

The target router's ISDN line information includes:

- The ISDN provider's switch type
- ISDN Directory Numbers (DNs)
- ISDN SPIDs
- Options (Lock Line Speed, etc.)

You must enter ISDN line information for your target router. All of this information is provided by your telephone company (refer to Chapter 1 for more details).

⇒ From Configuration Manager's main menu, click **ISDN Settings** and then click **ISDN Switch** to access the following window:

ISDN Switch

⇒ Specify the **Switch Type** that your ISDN service provider is using in the **Telco Switch Type** field. Select one of the appropriate switch:

NTT (Nippon Telephone and Telegraph)
KDD (Kokusai Denshin Denwa Co., Ltd.)
AT&T 5ESS custom
Northern Telecom DMS-100 custom
NI1 National ISDN 1 (compliant switches)
NET3 for European ISDN
NET3SW for European ISDN NET3 Swiss-variant

Note: NI1 is the most common and preferred switch type in North America.

Directory Numbers (DNs)

⇒ Enter directory numbers corresponding to the ISDN B-channels in the field labeled **ISDN DNs**.

SPIDs (North America only)

One ISDN SPID may be assigned for each B-channel of the ISDN line, or one SPID may be assigned for both channels, or SPIDs may not be provided at all. The SPID look like the Directory Number extended with additional digits.

Note 1: SPIDs do not apply to NTT, KDD, and NET switch types.

Note 2: Outside North America, SPIDs are not implemented.

Auto SPIDs detection

The router features an auto SPIDs detection program that attempts to collect telephone-related information automatically. In most cases, the telephone information will be detected successfully.

Note: If auto SPIDs detection fails, the user will have to enter this information manually.

Once you have set a switch type and directory numbers, the router can try to automatically detect the SPID numbers as follows:

⇒ From the **ISDN Switch Settings** window, click the **Auto SPIDs** button.

⇒ The **ISDN Auto SPIDs Configuration** screen will appear. The router will attempt to detect several common SPID formats and this process may take about one minute. If valid SPIDs are found, they will be saved in the router automatically.

⇒ Follow the instructions given on the screen carefully.

If SPIDs detection fails:
Click **Stop SPIDs Search** and you will return to the previous screen where you can manually enter the SPIDs information.

Outgoing Data Calls Allowed / Incoming Data Calls Allowed

⇒ You have the option to allow outgoing data calls or incoming data calls by checking the appropriate box. This setting will become active when you close the dialog box.

This feature is mainly intended for router models equipped with analog telephony features (POTS routers): it allows you to receive and place analog calls without incurring lengthy and expensive phone calls for data (because you are allowing calls to an outbound bridge, for instance).

Lock Line Speed

When this setting is enabled, the router places and receives calls at the speed of 56 kilobits per seconds, regardless of the speed setting in the remote database.
To lock the line speed at 56Kb/s, click **OK** to set the ISDN parameters.

For more information on this option, refer to *Lock Line Speed at 56Kb/s*, p.80.

Analog Phone Settings

Important: This feature only applies if you have a POTS router.

⇒ Click **Analog Phones** in **ISDN Settings**.

Your POTS router is preconfigured with default settings for your telephone interfaces. The default analog phone settings for POTS 1 and POTS 2 are:

- **Both** (Dial and Answer Mode)
- **Always (**for both Data Preemption and Automatic Preemption)

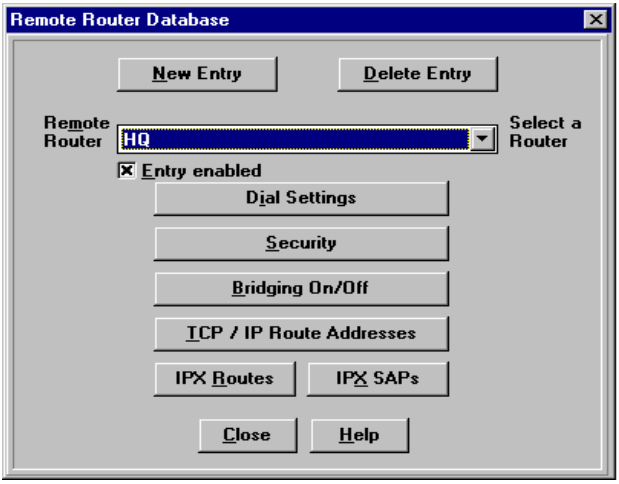
If you wish to change the default settings for the POTS interfaces, refer to *Analog Phone Settings*, p. 77.

Step 4. Remote Routers Database

Information about all the remote routers to which this (local/target) router may connect on the Wide Area Network (WAN) is entered into the router's remote router database. The remote router information includes:

- Dial settings
- Security
- Bridging specifications
- TCP/IP route addressing and protocol controls
- Remote IPX route services (IPX Routes - IPX SAPs)

⇒ Click **Remote Routers** from the main menu. This will open the **Remote Router Database** window.



Add, delete, modify, enable/disable an Entry

Add a New Remote Router

Before you enter your first remote router, the **Remote Router** field is blank. After adding a router, the screen displays as indicated above.

⇒ To add a new remote router to the remote router database, click **New Entry**. A new window opens (not shown).

⇒ Enter the new router name in the field provided and then click **OK**. The router name will then be placed in the list of routers, at the top of the list on the previous screen.

Delete a Remote Router Database Entry

⇒ Click the down arrow associated with the **Select a Router** field in order to display the list of remote routers entered into the database.

⇒ Click the name of the router entry you wish to delete. Click **Delete Entry**.

⇒ In the **Delete Entry** small window, confirm by clicking **Yes.**

⇒ Click **Close** to exit the **Remote Router Database** screen.

Modify a Remote Router Database Entry

⇒ Click the down arrow associated with the **Select a Router field** in order to display the list of remote routers entered into the database.

⇒ Click the router name of the router entry you wish to modify.

⇒ Then proceed to select the items to modify (like **Dial Settings, Security**, etc.). Click **Close** to exit the **Remote Router Database** screen.

Enable or Disable Remote Router Entry

Router entries and changes are enabled by default. However make sure that the **Entry Enabled** box is checked. Disabling and then re-enabling an entry requires a reboot unless you have not rebooted between the changes.

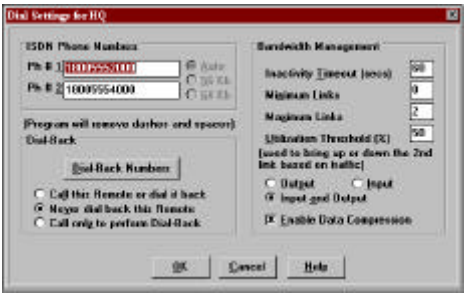
⇒ When you are done, click **Close** in the **Remote Router Database** window to return to the main window.

Dial Settings

After adding a router to the remote router database, you can then enter additional information about the router.

⇒ Click **Dial Settings.**

This next window allows you to set ISDN phone numbers for the remote router as well as control bandwidth management.



ISDN Phone Numbers

⇒ Enter one or two remote ISDN phone numbers associated with the remote router in the **ISDN Phone Numbers** field. This is the

number that will be dialed to connect to the remote router. (ISDN phone numbers can contain the numbers 0-9 and the characters * and #.)

Important: Be sure to include the area code and long distance prefix even if you are located in the same area code.

Dialing Speed

When placing an outgoing call to the selected remote site, you can adjust the bit rate of the call with one of three choices: 64 Kb, 56 Kb, or Auto.

Auto is the default mode: a 64-Kb-per-second call is attempted first with a fall back to 56 kilobits. You can, however, restrict the router to only dial at either 64 or 56 kilobits per second.

Bandwidth Management

Inactivity Timeout

⇒ Enter a number (in seconds) in the field labeled **Inactivity Timeout.**

This will force a disconnect and will minimize dial-up costs. (The default disconnect time is 60 seconds.)

The router will disconnect the ISDN link after the number of seconds has passed since the last data transmission.

Minimum Links

You can set the minimum number of links to be used for remote data transmission.

⇒ Specify a number of B-channels (up to maximum links) to be permanently allocated for the remote site connection or specify that a channel is allocated only as required. **(0** is the default indicating a channel is allocated when needed)

⇒ Specify **1** or **2** for permanent allocation of one or two channels.

Maximum Links

When traffic is sent or received, one or two channels can be used for data transmission. This configuration setting determines whether a maximum of one or two B-channels are available for remote transmission.

⇒ Enter **1** or **2** in the field labeled **Maximum Links**.

(The default is to have one channel or link available for the connection.)

Utilization Threshold (%)

Initially a call is activated on one B-channel. When bandwidth utilization reaches the bandwidth threshold, the second B-channel is activated (if the maximum links value has been set to 2). Both channels are utilized until the bandwidth utilization drops below the threshold for 5 seconds, then the second channel is dropped.

⇒ Set a number from **0** to **100** in the field **Utilization Threshold**.

(The default is 50% utilization which means that the second channel will connect immediately after the first channel connects.)

Bandwidth Management Direction

Bandwidth management can be applied to incoming, outgoing, or both directions of traffic between the router and the remote site.

Select **Input**, **Output,** or **Input and Output.**

Enable Data Compression

Compression for the link is enabled by default.

⇒ However, if you experience compatibility problems, turn off data compression.

Dial-Back Numbers

Dial-Back forces the local router to refuse an incoming call from the remote router and dial the remote router back. This feature allows ISDN phone charges to be billed to the local router. Check Chapter 6, *Advanced Configuration Features,* for additional information.

⇒ Click **OK** to save all of the remote router's dial settings.

Security Information

⇒ From the remote router menu screen select **Security.**

The **Security** window allows you to specify the type of authentication and password required by the target router when communicating with the remote router.

Security Authentication Protocol

The authentication protocol is the minimum security level that the target router must use when communicating with the remote router. This protocol level is checked during security negotiation. The Router will *always* attempt to negotiate CHAP, the highest level of security possible. The router will not accept a negotiated security level less than the minimum authentication level selected.

⇒ Click **CHAP**, **PAP**, or **None**. PAP is the default.

Note: The authentication process occurs regardless of whether a remote router has dialed in or the target router is dialing out, and even if the remote end does not request authentication. Authentication is a bi-directional process, where each end can authenticate the other using the protocol of its choice (provided the other end supports it). The parameter in the remote router database is the minimum security level used by the target router when challenging or authenticating the remote router.

Disable Authentication

⇒ Check the **Disable Authentication** box if you wish to prevent your router from authenticating the remote router when dialing out.

The router will not request any authentication information from the remote router, but will still reply to any PAP or CHAP authentication request performed by the remote, such as your ISP. When this setting is in effect, the selected remote will not be able to dial into your router since the router always requires authentication when accepting incoming calls.

Security Authentication Password

This password is the remote router's password used by the target router to authenticate the remote router.

⇒ To enter or change the remote router's password, click **Remote's Password**.

⇒ In the next window, enter a new password in the fields provided.

The password is not displayed as you enter it and must be entered twice. A new password overrides the previous one set. Blank passwords are not acceptable.

⇒ Click **OK** to set the password. Click **OK** again to save the security specification.

Bridging Capability

⇒ From the **Remote Router Database** menu screen, select **Bridging On/Off.**

You specify whether the target router bridges traffic to/from this remote router.

⇒ Click **On** or **Off** (default) to turn bridging on or off.

Spanning Tree Protocol (STP)

You can also specify if you wish the router to use the Spanning Tree Protocol (STP) which allows the router to check for bridging loops and communicate with other sites that support the protocol.

⇒ Select **On** or **Off.** Click **OK** to set the bridging parameters.

Default: The default behavior of the router is to NOT implement STP when bridging over the ISDN WAN. This eliminates a period of about 40 seconds during which the ISDN lines are dialed and no user traffic is forwarded, while the Spanning Tree Protocol checks for and eliminates loops in the network topology.

On: If there is a possibility of redundant paths between nodes, the Spanning Tree Protocol should be turned on when dialing a site where such a loop possibility exists.

Off: If you choose to leave STP off, this assumes that no pair of nodes on the larger network, made by joining all the local LANs that can dial each other, can be connected by more than one path. This assumption usually holds true for telecommuters and many branch office situations.

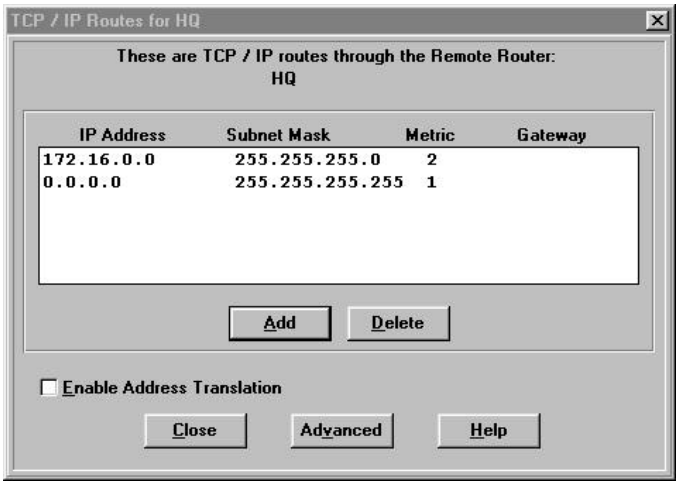
TCP/IP Route Addressing and IP Protocol Controls

TCP/IP Route Addresses

⇒ From the **Remote Router Database** menu screen, select **TCP/IP Route Addresses.**

If you are configuring TCP/IP Routing, you now need to enter details about routing to stations/networks on the LAN connected beyond the remote router. Refer to the section *Important Routing Concepts*, page 26 to determine if you need to seed the routing table and what information is required.

⇒ To seed the routing table, you will enter the **TCP/IP Route Addresses** into the table using this window.



This window displays a list of each network IP address with the corresponding subnet mask, metric, and gateway if needed.

The metric is a number between 1 and 15 that indicates the perceived cost in reaching the remote network or station.

⇒ To add a new entry, click **Add,** enter the IP address, subnet mask and metric in the small window displayed and click **OK**.

⇒ You must enter a default route for one remote router (if the target router will be placing calls to that remote router). The default route is specified as: **0.0.0.0 255.255.255.255 1** (or you may click the default route button).

Note: There can be only one default route specified for all the remote database entries. Defining a default route on the WAN is comparable to defining a gateway on the LAN.

If you have more than one router, be sure to choose only one router as the default router and change the configuration of the other routers accordingly.

Enable Address Translation

⇒ You will need to check this box if you are connection to an Internet Service Provider that has assigned you a single IP address.

Refer to *Network Address Translation* (NAT), page 72, for more details.

Source and Remote WAN IP Addresses

⇒ Click the **Advanced** button if you wish to specify WAN IP addresses or set IP protocol options.

You may need to specify a **Source WAN Port Address** and/or a **Remote WAN Port Address** for the WAN connection to the remote router, depending on IP address negotiation under PPP. Refer to the section *Important Routing Concepts*, page 26, to determine if you need to specify these addresses. Enter the IP addresses and corresponding subnet masks if required on this menu screen.

WAN RIP Settings (IP Protocol Controls)

For more information, refer to Chapter 5, *Configuring Advanced Features.*

IPX Route Addressing/Services

Skip to step 5, if you are not using IPX Routing.

⇒ From the remote router menu screen, select **IPX Routes.**
⇒

If you are configuring IPX Routing, you now need to enter details about routing to network segments connected beyond the remote router. Ask your network administrator to determine if you need to seed the routing table and what information is required.

IPX Routes

⇒ To seed the routing table, you will enter **IPX Route Addresses** in the **IPX Routes** window.

This window displays a list of each **IPX Network Number** with the corresponding **Hops** count and number of **Ticks**.

The IPX routes entered here may be to an internal or external network number depending upon how the router is being used.

The **Hop** count is a number greater than 1 representing the number of routers that must be passed through to reach the network number.

The number of **Ticks** indicates how much time that the packet takes to reach the network number in units of roughly 1/18th of a second. This number must be at least 1.

Note: ISDN lines can incur large delays, especially when dialing long distance. You can determine the actual delay by performing an IP **`ping`** and dividing the result by 2. A typical value is 50 ms (~3 ticks).

⇒ To add a new entry, click **Add,** enter the IPX Network Number, Hop Count, and Ticks in the small window displayed and click **OK**. (The **Tab** key can be used to tab between each item on the entry window.)

⇒ To delete any entry, click the line containing the entry, click **Delete** and click **OK** on the verification window.

IPX SAPs

If you are configuring IPX Routing, you will also need to enter details about services that are available on the LAN networks connected beyond the remote router.

Ask your network administrator to determine if you need to seed the services table and what information is required. To seed the services table, click **IPX SAPs**.

The window displays a list of each **Server Name** with the corresponding **Server Type, Network #, Node #,** and **Socket #**. The **WAN Network Number** is displayed.

⇒ To add a new server entry, click **Add.**

⇒ Select a server by entering the **Server Type**, click one of the servers already defined, or define your own.

⇒ In the following field, enter:

- Server Name (Service Name)
- Network number (The Network # is the 8-character hexadecimal internal network number associated with the server)
- Node Number (The Node # is the 12-character hexadecimal internal node number associated with the server entered in the format xx-xx-xx-xx-xx-xx)
- Socket number (The Socket # is the 4-character number representing the service (application) within the server node)
- Click **OK.**

Note: This information is available from your network administrator.

⇒ Seed the table with the **SAP** information of the primary logon server on the remote network. All other SAPs will be learned automatically. This entry is used for spoofing.

⇒ You can modify the **WAN Network Number** by clicking **Modify.**

Enter the 8-character hexadecimal network number for the WAN link and click **OK.**

Note: Only one router needs to define this. The other router will learn this.

Step 5. General Bridging and Routing Controls

⇒ To set bridging and routing controls and enable an Internet Firewall, click **Bridging/Routing** from the main menu.

Note: You should have already entered a remote router into the **Remote Router Database,** if you intend to perform outbound bridging.

Outbound Bridging

If you wish the router to perform outbound bridging, you must select a remote **Default Bridging** destination to be used on all dial-out operations.

⇒ Click the down arrow by the **Select Remote** field to display the list of routers in the Remote Router Database and select the router to be used for the remote router default bridging destination.

Be sure to enable bridging in the **Remote Router Database** for this remote router.

Note: Inbound/outbound bridging from/to specific remote routers can be disabled by setting bridging off in the **Remote Router Database**.

TCP/IP Routing

⇒ Set TCP/IP Routing to **On** or **Off**.

The default is TCP/IP Routing **Off**. If TCP/IP Routing is **Off**, then the Internet Firewall is forced inactive.

IPX Routing

⇒ Set IPX Routing to **On** or **Off**.

The default is IPX Routing **Off**.

Internet Firewall

⇒ Set the Internet Firewall to **On** or **Off.**

When the Internet Firewall is **On**, the router performs IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet. This filter discards packets received from the WAN, which have a source IP address recognized as a local LAN address.

WAN-to-WAN Forwarding

This option allows the user to manage data forwarding from one WAN link to another. WAN-to-WAN Forwarding is enabled by default.

You may want to disable this option, if, for example, the router is used at home to access both a company network and the Internet at the same time, and it is desirable that company information does not pass to the Internet.

Step 6. Store the Configuration

After you have followed steps 1-5, you are ready to save the configuration to FLASH in the router.

⇒ Click **Store** on the main menu. Click **OK** again to confirm the store operation.

Any settings that you have modified will be permanently stored in the router's configuration. Any settings you have not modified will be unchanged (or default if this is your first configuration). If you do not save the configuration to FLASH, the configuration is lost upon reboot or power down of the router.

You will be prompted to reboot the router (next step).

Step 7. Reboot the Router and PC

After storing the configuration, you will be asked if you wish to reboot the router.

⇒ Click **Yes** to confirm. A message window will inform you that router rebooting is occurring.

⇒ Click **Exit** to leave Configuration Manager.

If you are using IPX routing, bridging, or DHCP, you may need to also reboot PC clients so they can locate the new network segment or settings.

Step 8. Verify the Router Configuration

Before you proceed with testing your router configuration, verify your ISDN settings as follows:

⇒ In **Port Monitor**, are the two channels in " standby"?

⇒ If you have a POTS router, do you hear a dial tone when picking up the phone handset?

Test IP Routing

Test IP Routing over the Local Ethernet LAN

Use the TCP/IP **`ping`** command or similar method to contact the configured target router specifying the Ethernet LAN IP address.

If you cannot contact the router:

- Verify that the IP address and subnet mask are correct
- Check cable connections and pinning

Test IP Routing to a Remote Destination

You can verify IP connectivity to the remote by running a **ping** command from a local LAN-connected PC. You will probably find a ping utility bundled with your TCP/IP stack. In Windows 95 and Microsoft's TCP/IP 32-bit stack for Windows for Workgroups, the command is called PING.EXE and can be found in your Windows directory.

Note: Before using the **ping** command to troubleshoot, make sure that the PWR, LINE, and NT1 lights are green.

Start a DOS Window:

1. Select **Start** from the Windows 95 taskbar.
2. Select **Programs**.
3. Select **MS-DOS Prompt**.

Issue the PING Command:

In the DOS window, type the command:

`ping <IP address>`

Example: `ping 192.168.254.254`

When you enter the **`ping`** command, the router will dial out to the remote router using the ISDN line. ISDN Status LED CH1 or CH2 should go on.

If you cannot contact the router using the ping command:

- Run the **Port Monitor** to check the status of the ISDN channels (Refer to *Port Monitor*, page 83).
- If the ISDN link is not in standby mode, verify the target router's ISDN configuration, SPIDs and DNs, telephone company provisioning, associated equipment (NT1, etc.) and cable connections.
- If the ISDN line is operational, check the remote router's telephone numbers and links parameter.
- Check that, if required, you specified valid remote WAN IP address and local WAN IP addresses.
- Verify the security authentication method and password of the remote router. Also, the router's entry must be enabled.

Test Routing from a Remote Destination

Have a remote router contact the target router using a similar method and verify both ISDN B-channels.

Test TCP/IP Routes

Contact a station, subnetwork or host on the network beyond a remote router to verify the TCP/IP route addresses entered in the remote router database.

Test IPX Routing

Test IPX Routing to a Remote Destination

Check for access to servers on the remote LAN as follows:

- Use the 'NetWare Connections' selection provided with NetWare User Tools under Windows or issue the command '`pconsole`' under DOS.
- Select the printer server and verify that the server you have defined is listed. When you attempt to access the server, the router will dial out to the remote router using the ISDN line.

If you cannot access the remote server:

- Check that the local Ethernet LAN IPX network number is correct.
- Verify that the WAN link network number is the same as the remote WAN link network number.
- Check cable connections and pinouts.
- Verify that the IPX Routes and IPX SAPs you have specified are correct.

If you cannot contact the remote router, run the Port Monitor to check the status of the ISDN channels.

- If the ISDN link is not in standby mode, verify the target router's ISDN configuration, SPIDs and DNs, telephone company provisioning, associated equipment (NT1, etc.) and cable connections.
- If the ISDN line is operational, check the remote router's telephone numbers and link parameters.
- Verify the security authentication method and password of the remote router.

Step 9. Disconnect from the Router

⇒ You can release the connection between your PC and the target router at any time by clicking **Disconnect** on the main menu.

⇒ Click **Exit** to leave Configuration Manager.

⇒ If you change any of the router's configuration settings, be sure to store the configuration into FLASH memory and reboot the router.

Once you have rebooted the router, you will need to log in again if you wish to further change the configuration.

Sample Configuration

In this configuration example of a hypothetical network, a small office **(SOHO)** will access a central site **(HQ)** via an ISDN link. The small office also has access to Internet through an Internet Service Provider **(ISP).**

The small office, SOHO, has IP routing enabled to ISP with a Class C addressing scheme, and to HQ.

Bandwidth-on-Demand is configured for accessing central site HQ.

The default of one line is configured for calling the ISP (though two different phone numbers are defined for use).

DHCP server's IP addresses are used. DHCP will be set up to issue DNS information to the SOHO LAN.

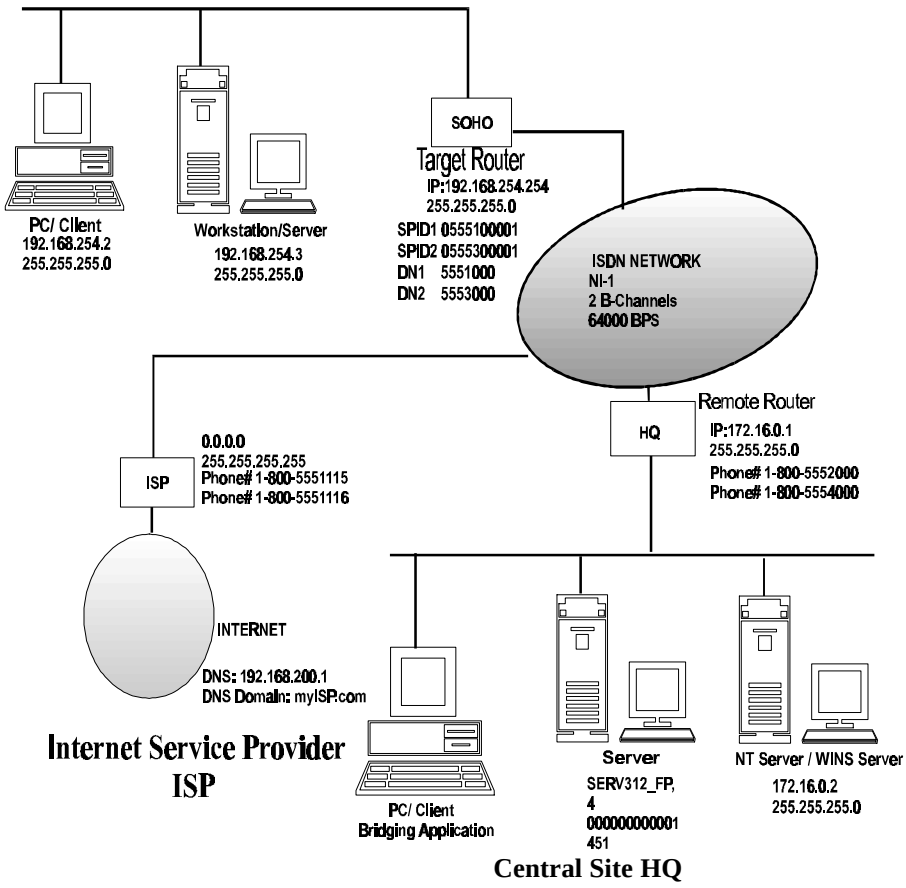
Network Address Translation (NAT) will be enabled to the ISP, since the ISP assigned SOHO only one IP address.

The following diagram and Network Information Worksheets show configuration of router SOHO at the small office.

Note: Blank Network Information Worksheets in Appendix C are available to enter information for your own configuration.

Sample Network Diagram

Small Office SOHO (Target Router)



Sample Network Information Worksheets

TARGET (local) ROUTER: SOHO		
Configuration Section	**Item**	**Setting**
System Settings	Router Name	**SOHO**
System Settings	Message	**Configured_JULY_1997**
System Settings Authentication Password	Dial Authentication Password	**SOHOpasswd**
System Settings DHCP Settings	Use defaults, but add: DNS Domain Name DNS Server WINS Server address	 **myISP.com** **192.168.200.1** **172.16.0.2**
ISDN Settings ISDN Switch	ISDN SPID#1 ISDN SPID#2 ISDN Directory Number #1 ISDN Directory Number #2 ISDN Switch Type	**0555100001** **0555300001** **5551000** **5553000** **NI1**

REMOTE ROUTER ENTRY: HQ		
Configuration Section	**Item**	**Setting**
Remote Routers Dial Settings	ISDN Phone #1 (11 digits) ISDN Phone #2 (11 digits) Inactivity Timeout Maximum Links Minimum Links Utilization Threshold Bandwidth Direction	**18005552000** **18005554000** **60** **2** **0** **75** **Input and Output**
Remote Routers Security	Minimum Authentication Disable Authentication Remote Router's Password/Secret	**None** **Yes** **Hqpasswd**
Remote Routers Bridging	Bridging On/Off Spanning Tree Protocol	**On** **Off**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metrics Address Translation In Advanced: Source WAN IP Address and Subnet Mask* Remote WAN IP Address and Subnet Mask*	**172.16.0.0 255.255.0.0 1** **Disabled** **Not required** **Not required**

* Used only in PPP numbered mode of addressing

Note: One chart for each remote router in the Remote Router Database

REMOTE ROUTER : ISP		
Configuration Section	**Item**	**Setting**
Remote Routers Dial Settings	ISDN Phone #1 (11 digits)	**18005551115**
	ISDN Phone #2 (11 digits)	**18005551116**
	Inactivity Timeout	**Default (60 seconds)**
	Maximum Links	**Default (1)**
	Minimum Links	**Default (0)**
	Utilization Threshold	**Default (0)**
	Bandwidth Direction	**In and Out**
Remote Routers Security	Minimum Authentication	**None**
	Disable Authentication	**Yes**
	Remote Router's Password	**ISPpasswd**
Remote Routers Bridging	Bridging On/Off	**Bridging Off**
	Spanning Tree Protocol	**Off**
Remote Routers TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metrics	0.0.0.0 255.255.255.255 1
	Address Translation	**Enabled**
	In Advanced: Source WAN IP Address and Subnet Mask*	**Not required**
	Remote WAN IP Address and Subnet Mask*	**Not required**

* Used only in PPP numbered mode of addressing

Note: One chart for each remote router in the remote router database

BRIDGING AND ROUTING CONTROLS		
Configuration Section	**Item**	**Setting**
Bridging / Routing	Default Remote for all dial outs	**HQ**
	TCP/IP Routing On/Off	**On**
	IPX Routing On/Off	**On**
	Internet Firewall On/Off	**On**

Names and Passwords Example

In the sample configuration provided, the small office SOHO communicates with the central site HQ and the Internet Service Provider ISP.

System Passwords

SOHO has a system password 'SOHOpasswd'. This password is used when SOHO dials out to site HQ for authentication by that site, and at any time when HQ challenges SOHO.

HQ has a system password 'HQpasswd' which is, likewise, used when HQ dials out to site SOHO for authentication by SOHO, and at any time SOHO challenges HQ.

ISP has a system password 'ISPpasswd' used for the same purpose.

Remote Passwords

Each router has a remote router's password for each remote router defined in its Remote Router Database. The router will use the remote password to authenticate the remote site when the remote router dials in or is challenged by the local site.

For example, SOHO has remote router entries for HQ and ISP, and defined in each entry are the respective remote router's password.

The following table shows the names and passwords for each router that must be defined for authentication to be performed correctly. (This assumes that all three systems use some form of authentication protocol.)

Note: If you have trouble with passwords, we recommend that you set the remote router security to "**disable authentication**" to simplify the process.

	Names & passwords configured in SOHO Router	Names & passwords configured in HQ Router	Names & passwords configured in ISP Router
System Name	SOHO	HQ	ISP
System Password	SOHOpasswd	HQpasswd	ISPpasswd
Remote Router Database	HQpasswd ISPpasswd	SOHOpasswd	SOHOpasswd

Chapter 5. Configuring Advanced Features

The features described in this chapter are advanced topics. They are primarily intended for experienced users and network administrators to perform network management and more complex configurations.

These following features are accessed and configured from Configuration Manager:

- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- IP Routing Controls (RIP)
- CallerID
- ISDN Dial-Back
- Telephone's Analog Settings
- Lock the ISDN line speed at 56 Kb/s

Dynamic Host Configuration Protocol (DHCP)

The router supports **DHCP**, and acts as a DHCP server itself, allowing hosts (PCs, etc.) to acquire initialization parameters (IP addresses, masks, domain names, etc.) automatically. These initialization parameters are collectively called the **lease** and are valid for a certain amount of time (usually one week). When a lease expires, a new one is acquired. For this to happen, your PC has to be configured to use DHCP.

PC Configuration

DHCP has to be enabled on your PC. The following instructions still assume a Windows 95 environment.

1. Follow the instructions in Chapter 1 (*Hardware Installation)* for connecting your network cables (single station configuration or hub configuration).
2. Power the router on.
3. On your PC desktop, click the **Start** button. Select **Settings**. Click **Control Panel**. Select **Network**.

4. If the TCP/IP stack is installed on your PC (it will be listed under **Configuration**), proceed to **step 5.**

   Note: If you do not have a TCP/IP stack installed on your computer, follow these instructions:

   a) In **Configuration,** click **Add**.

   b) In **Select Network Component Type**, click **Protocol** and click **Add.**

   c) In **Select Network Protocols**, under **Manufacturer***s*, click **Microsoft.**

   d) In the same **Network Protocols** window, click **TCP/IP**, and click **OK**.

5. Under **Configuration**, double-click **TCP/IP**. Select **Obtain an IP address** automatically.

   Note: If you are connecting to a Windows NT server:

   1. Click the **Wins Configuration** tab.
   2. Click **Use DHCP for WINS Resolution**.
   3. Click **OK.**

6. Click the **DNS Configuration** tab and select **Disable DNS.** Click **OK.**

7. You are now back in the **Network** window. Select the **Identification** tab.

   Enter a **computer name**, a **workgroup name**, and **computer description** if you wish. Click **OK.**

8. Files are now being copied.

   A "*Setting Changes*" message will ask you if you wish to restart your computer. Answer **Yes.**

   The PC has finished rebooting. It can now acquire its own IP address from the router using DHCP.

9. You now need to run Configuration Manager to enter the DNS and a domain name into the router. On the next boot, the PC will learn the DNS and Domain Name from the router.

Router Configuration

The following configuration instructions are intended for users who are primarily configuring their router for Internet access.

DHCP Settings

The router is preconfigured with a preset IP address pool and a gateway (192.168.254.254). Before becoming active, the router's DHCP server attempts to locate other active DHCP servers on the network such as Windows NT servers. If one is detected, the router's DHCP server disables itself.

This picture shows a DHCP sample configuration.

The DHCP Server Settings screen allows users to:

- Change the IP Address Pool if needed
- Configure DNS information specifically for Internet access
- Configure the WINS Servers settings if working with Windows NT

⇒ To access the **DHCP Server Settings** screen, click **System Settings** and **DHCP Settings**.

DHCP IP Address Pool

The existing IP Address Pool settings can be changed if you need to modify/increase the range of your address pool.

If you change your router's IP address, the router's DHCP server will automatically provide a new IP address pool for the new subnet if the preceding subnet was enabled.

DNS Configuration

If you intend to primarily configure your router for Internet access, you need to enter DNS information provided by your Internet Service Provider.

WINS Servers

If you work with Windows NT, you should enter your WINS Servers' IP addresses in the **WINS Servers** fields.

DHCP server is enabled

The router's built-in DHCP server might disable itself if another DHCP server (like a Windows NT server) is found on your local LAN, or if you manually disable it. If the DHCP server is disabled, all the other fields are greyed out.

Storing and Rebooting

Changing or entering new DHCP settings requires a **Store** in the router and a **Reboot** of the PC. This step is necessary so that the PC can acquire its initialization parameters from the router.

Note: Windows 95 users can easily acquire an IP address without restarting the PC using the **Winipcfg** utility as follows:

1. Click the **Start** button located on your PC desktop screen.
2. Click **Run**. Enter WINIPCFG.
3. Click **Release** to clear your current IP address and **Renew** to acquire new IP parameters. The new settings will be displayed.
4. Click **OK**.

Disabling DHCP

⇒ To disable DHCP, click the **Start** button on your PC desktop, **Settings, Control Panel**, and **Network.**

⇒ In **Network**, under the **Configuration** tab, double-click **TCP/IP**.

⇒ Select **IP Address** tab.

⇒ Select **Specify an IP Address**. Enter your PC's IP address and its subnetmask. Click **OK.**

⇒ Select the **DNS Configuration** tab.

Select **Enable DNS**. Enter the DNS information (check with your Network Administrator). Click **OK**. Click **OK** again.

Network Address Translation (NAT)

NAT is an IP address conversion feature that translates a PC's local (internal) address into a temporary global (outside/Internet) IP address.

NAT is needed when a PC (or several PCs) on a Local Area Network wants to connect to the outside Internet to get to a remote network: NAT swaps the local IP address to a global IP address. Our version of NAT goes one step further by allowing several PCs to share one single IP address to the Internet, thus reducing connection costs. In effect, it allows a whole LAN to connect to the Internet as a Single User.

Enable NAT

Important: Make sure that IP routing is enabled.

⇒ From the Configuration Manager's main menu, click **Remote Routers** and then **TCP/IP Route Addresses**.

⇒ In the **TCP/IP Routes** window, check the **Enable Address Translation** box.

Source and Remote WAN Port Address

This information is required if you are running NAT and the remote router does not dynamically assign the local/target router WAN Port Address. This address corresponds to the global IP address and is obtained from your Network Service Provider.

Most users do not need them as the router can automatically handle the numbered and unnumbered modes of IP address negotiation.

⇒ In the **TCP/IP Routes** window, click **Advanced**.

⇒ In the **Source WAN Port Address** window, enter the **IP Address** and its corresponding **Subnet Mask** and click **OK**.

Note: For information on WAN RIP settings, refer to the next topic, *Routing Information Protocol*.

Routing Information Protocols (RIP)

You can configure the router to send and receive RIP (Routing Information Protocol) packet information to and from, respectively, the remote router.

RIP is a protocol used by some routers to exchange IP routing information so that the local site will 'learn' all about the routes beyond the remote router and the remote router will 'learn' all about the local site's routes.

Note 1: You may not want this to occur in some cases. For example, if you are connecting to a site outside of your company such as the Internet, you may want to keep knowledge about your local site's routes private.

Note 2: With NAT (Network Address Translation) enabled, the local router cannot send RIP packets to the remote WAN link, but can, however, receive RIP packets from the remote site.

Default: The default is to restrict sending or receiving IP RIP packets or default routes. If RIP packets are not allowed to flow on the WAN link, you must seed the routing table. You can also advertise the remote site's existence. The default is to keep the remote site's existence private.

RIP Options

RIP-1 Compatible

In RIP-1 Compatible mode, the router can broadcast RIP-1 packets and multicast RIP-2 packets. It can also receive and interpret RIP-1 and RIP-2 packets.

RIP-1

It is used when exchanging RIP packets when communicating with older routers that don't have RIP-2. RIP-1 has the following two deficiencies: Since it uses broadcast for sending packets, every device on the LAN must receive and inspect every packet.

RIP-1 has no way of communicating a subnet mask. This deficiency can lead to misinterpretation of IP networks by the router receiving the RIP-1 packets.

RIP-2

RIP-2 lets the routers exchange subnet mask information in the packets.

Since it uses multicast addresses, only devices supporting RIP-2 will listen to RIP-2 packets.

Note: If your network does not support RIP, then use the RIP OFF option to turn it off.

Enable RIP Options

It is advisable to only turn RIP options ON when instructed to do so by your network administrator. Make sure that **IP routing** is enabled by clicking **IP and IPX Routing** from the main menu.

Note: RIP options do not apply to Bridging.

Turn on LAN RIP Settings

RIP-1 Compatible is enabled by default. To enable another RIP option:

⇒ From the Configuration Manager's main menu, click **System Settings** and then **Ethernet IP Address**. Your current IP Address and Subnet Mask are displayed.

⇒ Select the appropriate RIP options under **LAN RIP Settings**.

Turn on WAN Settings

RIP is disabled by default. To enable another RIP option:

⇒ From the Configuration Manager's main menu, click **RemoteRouters**. Select your remote router.

⇒ Click **TCP/IP Route Addresses**. In the **TCP/IP Route Addresses** window, click **Advanced**.

⇒ Select the appropriate RIP options under **WAN RIP Settings**.

Caller ID Security

Caller ID is an additional security feature on data calls supported by the router. It allows you to verify phone numbers of the remote routers when calls come in to the local router. You configure the phone numbers from which a specific remote router can call and enable or disable this feature systemwide. Any calls from other numbers will be rejected.

Note 1: Caller ID service (for the local router phone line) must first be obtained from the ISDN provider. 7 or 10 digits may be presented by switch.

Note 2: The configured phone numbers must contain the actual digits presented by the central office switch.

Enable Caller ID Security

⇒ To enable Caller ID Security systemwide, click **ISDN Settings** and check the box **Enable ISDN Caller ID Security**.

⇒ To specify unique numbers for the remote router, click **Remote Routers** and then **Dial Settings**. Check the appropriate radio button in the **Dial-Back** box.

⇒ Click **Dial-back Numbers** to add or delete remote routers' numbers.

⇒ Click **Store** to save the system settings and remote router database configuration.

⇒ Then test Caller ID: If the call is rejected by the local router, check the message displayed on the console message window in the Port Monitor or use the **`system history`** command for the actual digits received and reconfigure with the correct number.

ISDN Dial-Back

Dial-Back forces the local router to reject an incoming call from the remote router and to dial the remote router back. This feature is used to cause ISDN phone charge billing to the local router.

Dial-Back can be enabled, disabled, or enabled to only occur when the remote router calls first. When Dial-Back is configured, the local router's call delay timer setting must allow for disconnect and dial back; the defaults are 30 seconds for the U.S., and 90 seconds for Europe and Japan.

Dial-Back prerequisites

In order for ISDN Dial-Back to work, the following features have to be enabled:

- Caller ID must be provided by the ISDN provider for the line receiving the call (local router)

- The dial settings of the remote router need to be configured in the remote database of the local router.
- The remote router's phone number is entered in the remote database of the local router.

Configure Dial-Back

⇒ From Configuration Manager's main menu, click **Remote Routers** and then **Dial Settings**.

⇒ To add Dial-Back to a remote router, click **Dial-Back Numbers** in the **Dial-Back** box. In the new window, you may add or delete numbers.

⇒ You may now select one of the three Dial-Back options:

- **Call this remote or dial it back**

  This option lets the local router dial the remote router back or place a normal call to the remote router; in both instances, the local router will incur the charges.

  Note: This option requires Caller ID. It also requires that the ISDN network present the telephone number of the local router to the remote number. In certain areas, you may need to subscribe to this ISDN option with your ISDN provider.

- **Call only to perform Dial-Back**

  The local router can only dial back the remote router (right after the remote router has placed a call in). The local router cannot generate the phone call. The local router will incur the phone charges.

- **Never dial back this remote**

  This option disables Dial-Back: it is a normal situation where the router initiating the call, either the remote or local router, is responsible for the charges.

⇒ Click **OK** to enable your choice.

Analog Phone Settings

The following describes how to change the default settings of a POTS router (a router to which you may attach analog devices such as a telephone or a fax machine) for Analog Mode, Call Preemption, and Automatic Preemption.

Default phone numbers

The interfaces are preconfigured with the following default settings:

- If your ISDN settings are configured with two DNs (Directory Numbers), DN1 will be associated with POTS interface 1 and DN2 will be associated with POTS interface 2.
- Otherwise, the default configuration is for an incoming call to ring on all available devices attached to the POTS interfaces. An outgoing call will use any available B-channel.

Note: This default setting can be changed using the Command Line Interface but not Configuration Manager. Refer to Appendix D for instructions to access the Command Line Interface.

Phone usage and data preemption

Call preemption allows you to give voice calls priority over data calls: a voice call (depending on the configuration options) will cause a disconnect of a data call on an ISDN B-channel.

Default: The default configuration is for both incoming and outgoing voice calls to preempt data (**Always** option).

Data calls can be preempted manually or automatically. In manual preemption, data calls can be bumped manually by picking up the phone and depressing the flash hook to indicate that you want to preempt.

POTS line controls

Phone lines and data preemption can be controlled as explained in the following table:

Mode	Dial	This router can call out, but will not receive a call.
	Answer	This router can receive a call but cannot dial.
	Both	This router can call out **and** receive a call.
Voice Preempts Data	Always	If this router places **or** receives a call: voice always preempts data.
	Incoming	If this router receives a call: voice preempts data.
	Outgoing	If this router calls out: voice preempts data.
	Never	Voice will not preempt data.
Automatic Preemption Assumes that data preemption is enabled (in **Voice Preempts Data)**	Always	Automatic preemption applies for both outgoing and incoming calls
	Incoming	Automatic preemption applies for incoming calls Manual preemption applies for outgoing calls
	Outgoing	Automatic preemption applies for outgoing calls Manual preemption applies for incoming calls
	Never	Manual preemption applies for outgoing and incoming calls

Preemption Rules

- Voice calls always preempt data.
- Voice always preempts data if two B-channels are used for the same destination.
- Call preemption does not occur on incoming calls unless a person picks up the phone or the analog equipment answers the call.
- An incoming voice call may not always be forwarded from the central office if two B-channels are already in use for data calls. You must subscribe to a service called “Additional Call Offering” for the voice call to be forwarded to the router.

Configure Analog Phones Settings

Set POTS Interface Analog Mode

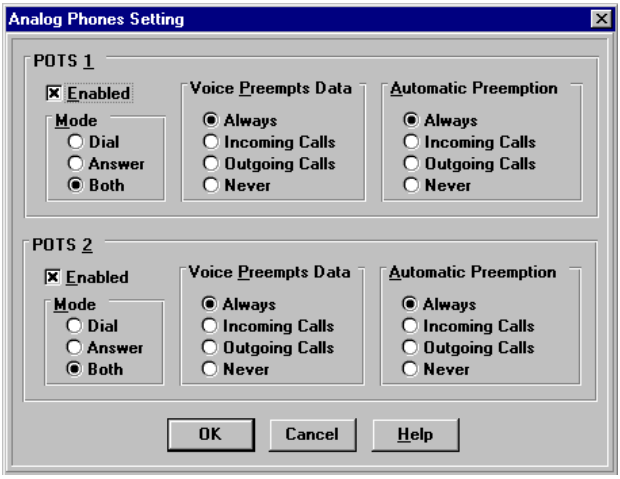
⇒ In **ISDN Settings**, click **Analog Phones**. In the **Analog Phones Setting** window, you may select one of these three options:

- **Dial**
- **Answer**
- **Both** (**Answer** and **Dial** are the default)

Voice Preempts Data

⇒ In **ISDN Settings**, click **Analog Phones**. In the **Analog Phones Setting** window, choose one data preemption option for each line:

- **Always**
- **Incoming Calls**
- **Outgoing Calls**
- **Never**



Automatic Preemption

⇒ In **ISDN Settings**, click **Analog Phones**. In **Analog Phones Setting**, you can select one of the following Automatic Preemption options:

- **Always**
- **Incoming Calls**
- **Outgoing Calls**
- **Never**

Note: To activate Automatic Preemption, Data Preemption has been already enabled.

Save and Test POTS configuration

⇒ Save the POTS configuration by clicking **OK** in the **Analog Phones Setting** window; then click **Store** in the main menu.

⇒ To test the POTS configuration, use the attached analog phone to dial out to a remote phone number and call attached analog devices from another phone.

Warning: If you do not save the configuration to FLASH, the configuration is lost upon reboot or power down of the router.

Lock Line Speed at 56Kb/s

This feature should only be used when a network operating at 56,000 bits per second actually signals calls at 64,000 bits per second. This feature forces all calls to 56,000 bits per second with rate adaptation.

⇒ To lock the ISDN line at 56,000 bits per second, click **ISDN Settings** from Configuration Manager's main menu.

⇒ Click **ISDN Switch**.

⇒ Put a check mark in the **Line speed locked at 56Kb/s** box to enable this option.

Chapter 6. Management Tools

This chapter describes tools designed to simplify file system management, software maintenance, and data traffic monitoring. These tools comprise:

- Terminal Window
- Port Monitor
- Upgrade/Backup
- Reboot from Network
- SNMP Options

⇒ To access these tools, click **Tools** from the main menu in Configuration Manager.

Terminal Window

The **Terminal Window** lets you access the **Command Line Interface (CLI)** through **Configuration Manager.**

Note: The CLI can also be accessed from a terminal emulation session running under Windows, from an ASCII terminal, or through a TELNET session for remote access.

How to access the Terminal Window

In order to access the Terminal Window, your PC or ASCII terminal must be connected to the **Console** port. All necessary information regarding accessing the CLI through Configuration Manager or through other modes of access is explained in details in Appendix D, *Accessing the Command Line Interface (CLI)*, page 119.

To open a Terminal Window session, click **Tools** from the Main menu and then **Terminal Window**.

Menu Selections

The **Commands** menu provides shortcuts to most of the commands described in the Command Line Interface. These shortcuts will substantially reduce the amount of typing. Click the commands that you need to enter them in the Window.

The **File** menu lets you open a **Log File** where all messages printed by the router on its console and all input performed directly at the console are recorded.

The **CommPort** menu allows the user to adjust the router's communication settings.

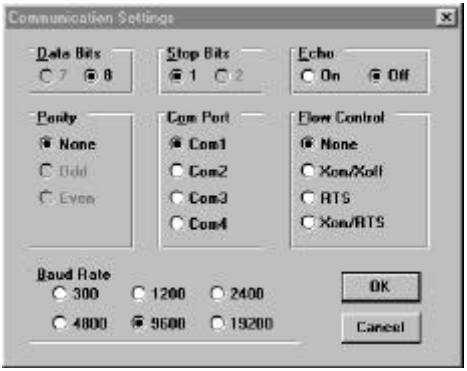
How to change the router's IP address using the Terminal Window

The user may wish to change the default IP address of 192.168.254.254 to a different address. This can be simply done using the Terminal Window to access the Command Line Interface.

The router's address is changed to be in the same IP subnetwork as the PC. However, the PC's address remains the same.

Instructions

1. The console (serial) cable allows you to access the Command Line Interface via Configuration Manager. Refer to Appendix D, *Accessing the Command Line Interface*, page 119 for installation and cable instructions.
2. Click the menu button **Tools** and then select **Terminal Window** to change the router's address.
3. Verify that the communication settings are set as shown in the picture below, and that the correct comport is selected.



4. In the terminal window, enter the following commands to set, save, and verify the router's LAN address and enable IP routing:

   `login admin` (`admin` is the default password)
   `eth ip addr` `x.x.x.x  y.y.y.y`

   where:
   `x.x.x.x` (IP address)
   `y.y.y.y` (subnet mask for the router's LAN connection)
   Ex: 192.168.254.254 255.255.255.0

   Note: Please refer to Appendix B, *Subnetwork Tables*, or ask your network administrator to determine which addresses are valid.

   `eth list`
   (This command lists the settings for the Ethernet LAN IP address and subnet mask as well as the port number)

   `save`
   `reboot`

5. Close the terminal window.
6. Click the **Connect** button in Configuration Manager.
7. Enter the same IP address you just assigned to the router.
8. Verify that you have set the router's LAN connection address and subnet mask correctly.

WAN Port Monitor

An ISDN port monitoring function is available to you, once you have connected to the router. If you use a router with POTS features, a POTS Monitor can also be displayed along with the ISDN Port Monitor.

Access WAN Port Monitor

Access from Configuration Manager

⇒ Connect to the router.

⇒ From Configuration Manager's main menu, click **Tools**.

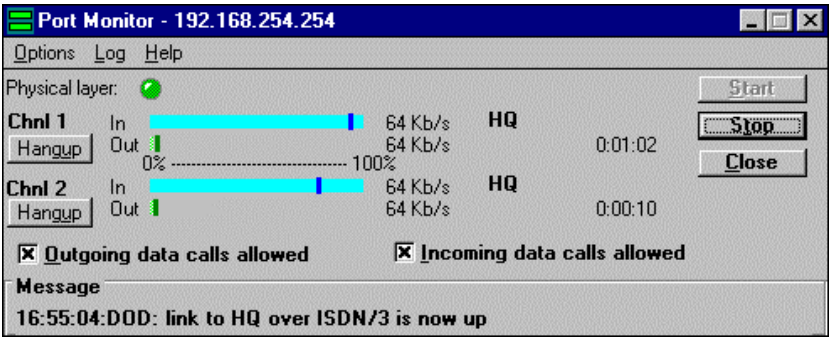
⇒ Click **WAN Port Monitor**. The ISDN Monitor will be displayed.

Access from outside Configuration Manager

Port Monitor is also a stand-alone application that can be launched outside of Configuration Manager as follows:

⇒ On your PC, click the **Start** button located on your desktop**.**

⇒ Click **Programs, Cabletron ISDN Tools,** and then click **WAN Port Monitor**.



Port Monitor Features

Message field

The ISDN Monitor window has a message field that displays the most current status message or error message read from the router.

Multiple monitor windows

Several ISDN monitor windows can be opened at the same time (by entering different IP addresses) to let you monitor different routers. You can also monitor routers, which do not reside on your LAN.

Display

When an ISDN B-channel is connected, the inbound and outbound bandwidth utilization of the channel is displayed. A vertical bar across the channel shows the average utilization (0-100%) and the bar length shows an instantaneous sample. The remote router name is also displayed.

The status indicator will let you know if the ISDN B-channels are out of service, in standby, ready, dialing, connected, closing, or accepting an incoming call.

⇒ Monitoring is continued until you click **Stop** or **Close.**

Physical layer

This light shows the status of the physical connection to the router.

Green light: the line is functioning correctly.

Red light: the circuit is either open or non-functional. Check your phone wiring and call your Network Service provider if you can not get a green light. This status correlates to the NT1 light on the router.

Hangup

To cause an ISDN channel to drop a data call, click the associated **Hangup** button. This feature is only available when there is a data call established to a remote router

Note that you can also prevent any future incoming or outgoing data call from being accepted or generated by clicking the corresponding check box.

Enable incoming and outgoing data calls

You have the option to allow or disable outgoing data calls or incoming data calls by checking the appropriate box. This feature is most useful for models equipped with analog telephony features as you may want to receive and place analog calls without incurring the risk of lengthy phone calls for data (because you are allowing calls to an outbound bridge, for instance).

Options

The **Options** menu allows the user to select the IP address or the monitoring frequency. It also provides a POTS monitor to look at the analog port activity or quit the application. The following describes the different available options:

Select Router
This option allows you to specify the IP address of the router you want to monitor. This setting is preserved in the file ROUTER.INI. When Port Monitor is started from Configuration Manager or Quick Start, the IP address of the router to monitor is the same as the one currently used by Configuration Manager.

Set Refresh Rate
This option lets you change the update frequency of the Port Monitor and POTS monitor windows.

By default, all information is refreshed once a second. If this causes strain on your network or you are presently monitoring a router across the WAN, which requires too much bandwidth usage to perform this function, you may want to increase the refresh rate, expressed in seconds.

Set Number of Display Lines

This option allows you to specify the number of lines of information that are shown in the Message area of the main Port Monitor window. However, you can obtain a more complete list of the messages generated by the router by using the Log window.
This setting is preserved in the file ROUTER.INI. Acceptable values are between 1 and 3. The default value for this setting is 1.

Set Display Clear Rate

This option allows you to specify how long, in seconds, the messages shown in the Message area of the Port Monitor main window are kept visible. After that time has elapsed (or whenever the monitoring is stopped), old messages are automatically erased to avoid confusion. You may, however, prefer to always be able to see the latest information generated by the router: To do so, set this parameter to a large number (3600 for one hour, for example).

View POTS

The POTS Monitor is integrated into the Port Monitor, but is only available with ISDN routers that support analog telephony features. It monitors the state of the two analog lines supported by the router and displays information for each one, including phone numbers for incoming and outgoing calls, and duration of calls.

Important: Incoming phone numbers can only be displayed if you have subscribed to the optional Caller ID service.

SNMP Options

For security reasons you may want to change the router's SNMP community name and UDP port number. By default the port number is 161 and the community name is the string "public".
For more information, refer to the SNMP Options section, page 90.

Exit

This selection terminates the monitoring and exits the Port Monitor application. The **Close** button of the main window has the same function. The next time you start the monitoring from its Program Manager group (or its Windows 95 Start Menu location), the same router will be monitored again.

If you have changed the incoming or outgoing data calls settings, you will be prompted to save your changes permanently. Since these settings take effect immediately, there is no need to restart the router after saving the changes.

Log

A logging function is available to see all the messages printed by the router on its console port (including any input performed directly at the console). You also have the option to save the content of the log window to a file of your choice: this is very useful to Technical Support.

When you click **Log Start**, you will prompted to supply the administrative password, if you have not done so already. When you close the log window or click **Log Stop**, the logging function is terminated and the log file, if any, is closed.

Upgrade/Backup

This menu gives you the options upgrade and backup or restore the following files:

- Firmware
- Script
- Configuration
- DHCP settings
- ISDN settings

Upgrade lets you upgrade or restore files from your PC to the router. With **Backup**, the files are downloaded from the router to your PC.

A TFTP utility, necessary to perform these operations**,** is integrated into Configuration Manager, but can also be used as a stand-alone application.

Instructions

⇒ Click **Tools** from the main menu and then click **Upgrade/Backup**.

⇒ Select one of the five options (Firmware, Script file, Configuration, DHCP Settings, ISDN Settings) and click **Upgrade** (or **Execute** or **Restore** depending on the files you have selected) or **Backup**.

A window will appear and give you the following default files in the name box:

- For Firmware, the default file is KERNEL.100
- For Configuration, the default file is SYSTEM.CNF
- For ISDN, the default file is ISDN.DAT
- For DHCP, the default file is DHCP.DAT

Note: the script file name is defined by the user.

⇒ Click **OK** if the displayed file name is right.

⇒ Otherwise select the proper file and directory from the list below the name box and click **OK**.

Upgrade/Backup Options

Upgrade/Backup Firmware

The firmware (kernel) resides in the router. It is automatically backed up to your PC, when you first connect to the router.

Upgrading the Firmware should only be done when advised by Technical Support or when you are installing a new version/upgrade of the router's firmware.

Execute/Backup Script file

This feature is used to load batch files of configuration commands into the router. This allows for customization and simpler installation of the router. A script file can contain commands, comments (lines introduced by the # or ; characters) and blank lines.

The file is created on your PC using Notepad or other text editor. The command syntax can be found in the Command Line Reference.

Execute a Script file

⇒ Select **Tools, Upgrade/Backup, Script Files**.

⇒ Click **Execute** and choose the script file you just prepared.

⇒ When you click **OK**, the script file is loaded to the router (under the name AUTOEXEC.BAT) and the router is restarted, thus executing the script.

Backup a Script file

⇒ Select the **Tools, Upgrade/Backup, Script Files**. Click **Backup**. The Script file is backed up from the router to your PC.

⇒ When you click **OK**, the file named AUTOEXEC.OLD is copied back to the router.

Upgrade/Restore Configuration files
A Backup or Upgrade operation on the configuration files will include all of the system configuration data, except ISDN or DHCP settings files.

Upgrade/Backup ISDN settings or DHCP files
Backing up or upgrading the target system ISDN settings file or DHCP file will respectively involve only the target systems ISDN settings file or only DHCP file. The files will be copied to the directory C:/CFGMGR by default.

Reset defaults

This feature allows you to clear all of your configuration files (ISDN.DAT, SYSTEM.CNF, DHCP.DAT) and to go back to the original factory default settings.

⇒ Click **Reset Defaults**. A message will ask you if you want to clear your configuration files.

⇒ If you answer **Yes**, the router will reboot.

Note: It is recommended that you back up all of your existing configuration files before resetting the defaults in your router.

Reboot from Network

Reboot from Network is used in the following situations:

- To perform Beta testing (e.g., testing new router software before downloading to FLASH memory)
- To allow several routers to reboot from the same file on a server

Rebooting from the network will upload the file you have specified into the router and execute it.

Note 1: KERNEL.100 is the default file and is installed under the default directory C:\CFGMGR or wherever you may have installed Configuration Manager.

Note 2: A Trivial File Transfer Protocol (TFTP) utility is built into Configuration Manager and is capable of reading from and writing to the network.

Instructions

⇒ To reboot from the network, click **Tools** from the Configuration Manager's main menu and then click **Reboot from Network.**

A new window will appear and let you select the file to boot from, in the file name box. KERNEL.100 is the default file.

⇒ Click **OK** to enable your choice.

⇒ Enter your login password and click **OK**.

SNMP Options

The router is preconfigured with the following SNMP default settings:

- **public** for the Community Name
- **161** for the UDP Port

You may, however, want to change the default settings for security reasons or to allow SNMP monitoring of a device located on the LAN while running NAT; both the device and the router can be monitored or managed at different UDP ports. Changing the settings will affect only the Windows configuration parameters but will not change the actual settings in the router.

The router values can only be changed with the Command Line Interface using the `system snmpport` or `system community` command.

Instructions

⇒ Click **Tools** and **SNMP Options.**

⇒ You may set the **UDP Port** to any number between 1 and 65,535. Make sure that the port you select does not conflict with another defined port.

⇒ The **Community Name** can be a string of up to 40 characters. Special characters are allowed.

Chapter 7. Router Feature Descriptions

The router supports the following industry standard protocols, security features, compression algorithms, and network management tools to ensure interoperability with other vendors' equipment.

Important: For router software references, consult the model-specific Quick Start Guide.

- IEEE 802.3 Ethernet
- Point-to-Point Protocol (PPP)
- Password Authentication Protocol and Challenge Handshake Authentication Protocol (PAP/CHAP)
- ISDN BRI
- Bridging, Routing, IPX Routing
- IEEE 802.1D Bridging
- Bridging and Routing Protocol Filtering
- Bandwidth-on-Demand
- POTS Analog Line Interface
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- Software upgrade utilities
- TELNET
- Windows GUI Configurator
- Command Line Interface

IEEE 802.3 Ethernet

The router provides a standard 802.3 Media Access Control layer for CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Ethernet communications.

Point-To-Point Protocol (PPP)

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. It is suitable for both high-speed synchronous ports as well as lower speed asynchronous dial-up ports. With this protocol, options such as security and network protocols can be negotiated over the connection.

The Router supports synchronous PPP over the ISDN port.

In **Single Link Mode**, PPP utilizes one ISDN B-channel for data transmission. PPP can be run over each ISDN B-channel for two separate conversations (split B-channel).

In **Multi-Link Protocol Mode** (MLP), PPP can simultaneously send and receive data over two ISDN B-channels on the same connection to optimize bandwidth usage.

The STAC® Electronics Stacker LZS™ Compression Protocol is supported over PPP providing up to 4:1 data compression.

The Ascend and Microsoft variants are also supported.

PAP and CHAP Security

The router supports the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP.

PAP provides verification of passwords between routers using a 2-way handshake:

One router (peer) sends the system name and password to the other router. Then the other router (known as the authenticator) checks the peer's password against the configured remote router's password and returns acknowledgment.

CHAP is more secure than PAP as unencrypted passwords are not sent across the network. CHAP uses a 3-way handshake:

One router (known as the authenticator) challenges the other router (known as the peer) by generating a random number and sending it along with its system name. The peer then applies a one-way hash algorithm to the random number and returns this encrypted information along with its own system name. The authenticator then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends.

ISDN

ISDN provides an inexpensive switched digital access to remote sites. The ISDN BRI standard provides for:

- Two high-speed 64Kbps bearer (B) channels used for voice or data connections
- One 16Kbps signaling data (D) channel used for call set-up, signaling, and other information

ISDN allows all types of information to be transmitted including voice, data, fax, and video. Multiple devices can be linked to a single ISDN connection, each having their own telephone number. Two or more channels can be combined into a single larger transmission pipe offering variable transmission speeds.

The Router supports one ISDN BRI line and either or both of the B-channels for transferring data. Voice is transferred using either B-channel. If the two B-channels are used for separate connections, each provides up to 64Kbps transfer rates. Both channels can be used together to provide uncompressed data transfer at up to 128Kbps. The router can also transfer compressible data at up to 512Kbps.

A **Network Terminator device** (NT1) provides the interface between ISDN terminal (router) equipment and the ISDN service provider. In North America, the NT1 is provided by the customer; outside North America, the NT1 is provided by the ISDN service provider. The Router comes with a built-in NT1 (U interface).

Telephone Switch Support

The telephone switch types supported in North America include:

- AT&T 5ESS custom
- Northern Telecom DMS-100
- Switches providing National ISDN 1 (NI-1) support

Outside of North America, the supported switch types are:

- NET3 (European ISDN)
- NET3SW (European Swiss-variant)

- NTT (Nippon Telegraph and Telephone)
- KDD (Kokusai Denshin Denwa Co., Ltd.)
- HSD64 (64Kb permanent connection)
- HSD128 (128Kb permanent connection)

Support for additional switches will be announced from time to time.

Bridging and Routing

Bridging

Bridging connects two or more LANs together so that all devices share the same logical LAN segment and network number. The MAC layer header contains source and destination addresses used to transfer frames. An address table is dynamically built and updated with the location of devices when the frames are received. Transparent bridging allows locally connected devices to send frames to all devices as if they are local.

Bridging allows frames to be sent to all destinations regardless of the network protocols used. It allows protocols that cannot be routed (such as NETBIOS) to be forwarded and allows optimizing internetwork capacity by localizing traffic on LAN segments. A bridge extends the physical reach of networks beyond the limits of each LAN segment. Bridging can increase network security with filtering.

Routing

Routing provides a way to transfer user data from source to destination over different LAN and WAN links using one or more network protocol formats. Routing relies on routing address tables to determine the best path for each packet to take.

Routing tables can be seeded; i.e., addresses for remote destinations are placed in the table along with network address masks and a metric for path latency. Routing tables are also built dynamically; i.e., the location of remote stations, hosts and networks are updated from broadcast packet information.

Routing helps to increase network capacity by localizing traffic on LAN segments and reducing the amount of broadcasts that would result from bridged traffic. It also provides security by isolating traffic on segmented

LANs. Routing extends the reach of networks beyond the limits of each LAN segment.

Bridging and Routing

The Router can operate as a bridge, as a router, or as both (sometimes called a brouter). The router will operate as a router for network protocols that are supported when routing is enabled. The router will operate as a bridge when bridging is enabled. When both bridging and routing are enabled, routing takes precedence over bridging; i.e., the router uses the packet's protocol address information to route the packet; if the protocol is not supported, the router will use the MAC address information to bridge the packet.

Operation of the Router is influenced by routing and bridging controls and filters set during router configuration as well as automatic spoofing and filtering performed by the router. General IP or IPX routing, and routing or bridging from/to specific remote routers are controls set during the configuration process.

Spoofing and filtering, which minimize the number of packets that flow across the WAN, are performed automatically by the router. For example, RIP routing packets and certain NetBEUI packets are spoofed even if only bridging is enabled. For more detailed information on packet routing and bridging, refer to the section *Routing and Bridging Operation* in the *Command Line Interface* guide.

IEEE 802.1D Bridging

The Router supports the IEEE 802.1D standard for LAN to LAN bridging. Bridging is provided over PPP as well as adjacent LAN ports. The bridging software uses transparent bridging. Configured as a bridge, the unit bridges data packets to the destination, regardless of the network protocols used.

Also included is the **Spanning Tree Protocol** allowing the Router to interoperate with other vendors' bridge/routers. This is a learning bridge; i.e., the bridge builds and updates an address table with each MAC source address and associated information when the packets are received.

IP Routing

IP routing support provides the ability to process TCP/IP frames at the network layer for routing. IP routing support includes the Routing Information Protocol (RIP) which allows the exchange of routing information on a TCP/

IP network. The router receives and broadcasts RIP messages to adjacent routers and workstations. Since IP sends out periodic RIP frames that could keep dial-up links permanently connected, filtering and spoofing are performed to minimize these broadcasts on the WAN links. The router uses the 'piggyback method' to send RIP update packets to the WAN port. The piggyback method means that RIP update packets are sent only when the dial-up link is established because of data traffic.

IPX Routing

Internetwork Packet Exchange (IPX) Routing support provides the ability to process IPX frames at the network layer. This support includes the Routing Information Protocol (RIP)* which allows the exchange of routing information on an Internetwork, and the Service Advertising Protocol (SAP), which provides a means of exchanging Internetwork service information. The router receives and broadcasts RIP and SAP messages to adjacent routers and workstations so that clients on the network can determine what services (file, print, etc.) are available on the network and obtain the Internetwork address of the servers.

Since IPX sends several types of control packets that could keep dial-up links permanently connected, control of updates, and spoofing techniques are employed to reduce this traffic. Specifically, RIP, SAP, Watchdog, and serialization frames are filtered and spoofed. RIP and SAP update frames are only sent piggybacked with data packets. SAP requests for the nearest server are spoofed, serialization frames are dropped, and Watchdog frames are spoofed.

* IPX-RIP is similar to IP-RIP except IPX-RIP includes a time delay in addition to a hop count

Bridging and Routing Protocol Filtering

Filtering can be used to allow efficient usage of network resources and provide security for your network and hosts.

IP Internet Firewall

The router supports IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet. A security violation can occur when a packet is received from a WAN link, typically connected from the Internet, which has the source IP address of a secure host on your LAN. Using this secure host address, functions can be performed which only the secure host is authorized to perform. This filter discards packets received from the WAN which have a source IP address recognized as a local LAN address.

Note: Most routers' Firewall implementations protect against one form of intrusion. The built-in protection Firewall of the router does not take the place of a professional Firewall system designed to protect against multiple violations.

Bridge Filtering

Bridge filtering allows a network administrator to control the flow of packets across the router. Bridge filtering can be used to 'deny' or 'allow' the transmission or reception of packets based on a 'matched pattern' using a specified position and hexadecimal content within the packet. Common uses are to prevent access to remote networks, control unauthorized access to the local network and limit unnecessary traffic. (This feature is configured through the Command Line Interface.)

Bandwidth Optimization Features

The router provides a number of features to maximize throughput and minimize usage of WAN resources.

Data Compression

The router supports data compression of up to 4:1 allowing data transfer rates over an ISDN line at up to 512Kbps.

Dial-on-Demand

Dial-up WAN resources are accessed only when remote access is required and released as soon as the resource is no longer needed.

Bandwidth-on-Demand

The router can optimize the use of WAN resources (i.e., two ISDN B-channels) to increase throughput, depending on load requirements. Two ISDN B-channels can be "bundled" to permit transmission of data traffic over both channels after a link utilization threshold is reached. The second channel is released when utilization falls below the threshold. Support includes both routing and bridging applications. Bandwidth-on-Demand management can occur on incoming, outgoing, or both directions. The Multi-Link Protocol for PPP (MLP) is used to implement this feature.

Split B-Channels

Each 64Kbps ISDN B-channel can be used individually for a separate data connection.

POTS Analog Line Interface

The router software support for local analog phone devices provides emulation of central office voice services to control the analog lines. Call progress tones and DTMF are supported. Only one line can dial at a time; the other line can have an established call in progress while the second line is dialing.

Simple Network Management Protocol (SNMP)

The router provides SNMP agent support and support for standard as well as Enterprise Specific MIBs. SNMP is also used internally for configuration of the router. The active SNMP agent within the router accepts SNMP requests for status, statistics, and configuration updates. Communication with the SNMP agent occurs over the LAN or WAN connection. Any management application using SNMP over UDP/IP (User Datagram Protocol/Internet Protocol) has access to the local SNMP agent.

The following MIBs are supported:

- MIB II
- Bridge MIB
- Ethernet MIB
- IP Forwarding MIB
- PPP MIB For LCP
- Enterprise MIB for configuration

Dynamic Host Configuration Protocol (DHCP)

DHCP is used to acquire IP addresses and options (such as the subnet mask, DNS, gateway, etc.) automatically. On the practical level, acquiring these initialization parameters with DHCP translates into avoiding the more involved router/PC process (reconfiguration of router and/or PC addresses to be in the same network).

Network Address Translation (NAT)

NAT is an IP address conversion feature that translates a PC's local (internal) address into a temporary global (outside/Internet) IP address.

NAT is needed when a PC (or several PCs) on a Local Area Network wants to connect to the outside Internet to get to a remote network: NAT swaps the local IP address to a global IP address. Our version of NAT goes one step further by allowing several PCs to share one single IP address to the Internet, thus reducing connection costs. In effect, it allows a whole LAN to connect to the Internet as a Single User.

Software Upgrades

Software upgrades can be performed remotely using the TFTP protocol for the software download process. The router's file system is a DOS-compatible file system and any file contained within the system may be retrieved or replaced using the TFTP protocol. Specifically, configuration files and operating

system upgrades can be updated. Chapter 6, *Management Tools*, describes how to upgrade software, boot the router from the network, make copies of configuration files, and perform other maintenance procedures. A TFTP server is provided with the software.

TELNET

TELNET access to the router is supported. TELNET allows you to log into the router as if directly connected through the console port. In this manner you can issue commands, using the Command Line Interface, to configure the router and perform status monitoring from any remote location. Any of the available TCP/IP packages containing the TELNET application can be utilized. Refer to the *Command Line Interface* for more information.

A special feature, **History Log**, described on page 110, allows the redirection of all console output (including notifications that would only appear at the console terminal) to any TELNET session.

Windows GUI Configurator

A Microsoft® Windows™-based program, Configuration Manager, is provided for configuring the router. This Windows GUI point-and-click configurator is described in the chapter *Installing and Accessing Configuration Manager*. A Winsock-compliant TCP/IP stack must be installed on your PC to run Configuration Manager.

Command Line Interface

Configuration is also supported through the Command Line Interface. This interface provides the ability to configure the same basic features as the Windows GUI configurator, but through the console port or Telnet. It also gives you the following capabilities:

- PPP Call Back
- Online status commands and error message monitoring
- Statistics
- Unique PAP or CHAP authentication or system name passwords

- Configuration of advanced features such as:

  Bridge filtering
  ISDN subaddressing
  Optional IP filters
  Optional encryption
  Advanced DHCP settings
  Additional security
  IP host mapping

These topics are discussed in the *Command Line Interface* guide.

Chapter 8. Troubleshooting

Investigating Hardware Installation Problems

Check the LEDs to solve common hardware problems

Power light is off

- Check that the power cord is firmly plugged into the back panel of the router and the other end into an active AC wall or power strip outlet.
- Check that the power switch is turned on.

LEDs are flashing

- The power up test has discovered a hardware error and the rightmost five LEDs flash an error code. Contact Technical Support.

ISDN NT1 channel LED is off/blinking slowly (North America only)

- This LED is only active if an NT1 is installed. If the unit has an internal NT1, a problem is occurring in the connection to the network.
- Examine the phone line cable for frays. Check that each end is securely plugged in.
- Contact the ISDN service provider to ensure the ISDN line is operational. If you have other ISDN equipment that is operational, temporarily plug it into the wall jack to verify the ISDN line out to the service provider.

ISDN NT1 LED is fast blinking

- The router NT1 is having trouble negotiating the ISDN U interface layer 1 protocol with the central office.
- Check the connection cables.

ISDN line LED is off/blinking slowly

- **Unit with a U interface**: a problem is occurring in the negotiation to the network.
- **Unit with an S/T interface**: a problem is occurring in either the connection to the external NT1 or the connection to the network. To ensure that an installed NT1 is operating properly, check the NT1's operational light. Refer to documentation supplied with the NT1 unit.
- Examine the phone line cable for frays. Check that each end is securely plugged in.
- Contact the ISDN service provider to ensure the ISDN line is operational. If you have other ISDN equipment that is operational, temporarily plug it into the wall jack to verify the ISDN line out to the service provider.

ISDN line channel LED is fast blinking

The router is having trouble negotiating SPIDs and DNs with the central office.

Problems with the terminal window display

- Ensure your console is plugged in and turned on.
- Verify that you are on the right communications port (com1, com2)
- Check the configuration parameters for speed, parity, etc. Make sure the console is not in an XOFF state. Try entering a '**ctrl q**'.
- Verify that the RS232 device attached to the console is configured as a 'DTE'. If not, a crossover or null modem adapter is required.

Problems with the factory configuration

- Compare the router configuration with your router order.
  Check the following items:
- Either **`ISDN BRI(S/T)`** or **`ISDN BRI(S/T and U)`** should be indicated in the **`Interfaces detected`** message during boot of the router. One or two RJ45 ISDN ports are provided on the rear panel.

- Verify that the model number is correct (displayed during the boot procedure). The model number (and serial number) is also displayed on the main window of Configuration Manager.

Investigating Software Configuration Problems

Problems connecting to the router

If you cannot connect your PC to the target router for configuration:

- For a LAN connection, verify that the router's IP address matches the IP address previously stored into the router's configuration.

  You must have previously set the router's Ethernet LAN IP address and subnet mask, saved the Ethernet configuration changes, and rebooted the router for the new IP address to take effect.

- Check that your LAN cable is pinned correctly and each end securely plugged in.

- Make sure the PC and target router are on the same IP subnetwork or the target router is reachable through a router on your LAN. They can, however, be on different networks if IP routing is off.

- Check Network TCP/IP properties under Windows 95 and the control panel of the TCP/IP driver installed under Windows 3.1.

- Check if the LAN LED on the router's front panel blinks when 'pinged'.

- Check your Ethernet board IRQ settings: the PC's table may become confused. If it is the case, reboot your PC.

Problems with the Login Password

You have been prompted for the login password and received the following message: "Login Password is invalid".

- Re-enter the correct password and hit enter. Remember that the password is case-sensitive. Check that you are entering *admin* in lowercase and that the Caps key is not active.
- If you have forgotten the password, you must reset the login password. Refer to the appendix A, *Changing Configuration Switches,* and perform the following procedure:

  1. Move switches **5** and **6** down.
  2. Type **`login`** *`newpasswd`*. Password checking is overridden.
  3. Move switches **5** and **6** up**.**
  4. Complete any configuration update that caused the prompt for login.
  5. Change your login password to a new password.
  6. Store the configuration and reboot the router.

Note: If you have not reset switches **5** and **6** up and have rebooted, you will place the router in maintenance mode. Set switches **5** and **6** up and turn the power off and then on.

Problems accessing the remote network

- Start the Port Monitor and check the status of the ISDN B-channels which should be in "Standby" mode.
- Check that the ISDN line SPIDs and DNs (if required) are valid, the telephone switch settings are correct and the line can be activated.
- Verify that the ISDN phone numbers are correct for the remote router.
- If you are not using the supplied ISDN cable, check that the cables are pinned correctly.
- Verify that PAP/CHAP passwords are correct. Ensure that the remote router operates at the same minimum level of security that you have set in the target router.

If Bridging

- Check that the Bridging Default Destination has been set.
- Check that bridging to/from the remote router is set on.
- Be sure to reboot if you have made any bridging destination or control changes.

If TCP/IP routing

- Check that TCP/IP Routing has been set on and is enabled at the remote end.
- Check that the IP address of the LAN beyond the remote router is correct, as well as the associated subnet mask.
- If the remote router WAN IP address and subnet mask are required, check that they have been specified correctly.
- Check that, if required, the source and remote WAN IP addresses are on the subnetwork.
- Check that you have seeded the routing table with a route or a default route, if RIP is not allowed to flow on the WAN link.
- Be sure to reboot if you have made any IP address, control or protocol option changes.

If IPX routing

- Check that IPX Routing has been set on and the remote end is enabled for IPX routing.
- Validate that the IPX WAN network number matches the remote router's WAN network number.
- Check that the IPX Routes (network numbers, hops, and ticks) seeded into the routing table for network segments and servers beyond the remote router are correct.
- Check that IPX SAPs correctly identify the servers and applications on the remote network and have valid network numbers, node numbers, etc.

Problems dialing

Remote router won't dial

- Verify that it has a default IP route or a default bridge.
- Check that the remote router is not disabled or in Dial-Back only and has a phone number.
- It may not be in standby due to ISDN problems.
- Verify if it is in standby mode.

No POTS dial tone

- ISDN link is not completely defined and is not in *Standby* mode.
- The POTS line is set to *Answer* only, is disabled, or is busy with data, and preemption is off.
- The phone is not plugged in.

Problems with bandwidth management

ISDN Channel 2 does not support overflow for channel 1

- Verify that the maximum links to the remote router is set to 2.
- Verify that Bandwidth-on-Demand has been set for the direction of traffic.
- Check that there are two phone numbers to the remote router.

Both ISDN channels are always used for traffic on connection to the remote router

- Verify that the bandwidth threshold is set > 0%.
- Check maximum and minimum link settings.

Diagnostic Tools

Troubleshooting Help File

The Configuration Manager's **Help** file features an extensive troubleshooting section which is meant to help you diagnose and solve problems quickly through a logical process of elimination.

This **Troubleshooting** file is also available as a freestanding application from the Start menu.

⇒ To access it, click the **Start** button on your PC desktop, click **Programs**, **Configuration Manager**, and double-click **Troubleshooting**.

ISDN Q.931 Cause Values

ISDN link level error messages include the Q.931 cause value. The cause value displayed is the cause number exactly or the number +128. The following table is a reference list of the Q.931 cause values.

Cause No.	Cause Name
1	Unassigned (unallocated) number
2	No route to specified transit network
3	No route to destination
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	User alerting, no answer
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format (incomplete number)
29	Facility rejected
30	Response to STATUS INQUIRY
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit/channel not available
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identify in use
85	No call suspended

86	Call having the requested call identity has been cleared
88	Incompatible destination
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiration
111	Protocol error, unspecified
127	Internetworking, unspecified

History Log

The **History Log** utility is a troubleshooting tool which displays the router's activity. It can be accessed from a terminal emulation session (including Configuration Manager) or from Telnet.

1. If accessing the logging utility through Telnet, click **Connect** from the menu, **Remote System,** and enter the router's IP address. Click **Connect.**

   If accessing the logging utility through Configuration Manager, select **Tools** and **Terminal Window** (the console cable is required).

2. Log in with your administration password into the router (e.g. "admin").
3. Use the command **`system history`** to view the buffer contents.

Other logging commands:

- If you wish to monitor your router activity at all time, enter the command **`system log start`** to view a continuous log, if you are using Telnet. (This command will not work in a Terminal Window session, but only from Telnet.)
- The command **`system log status`** is used to find out if other users, including yourself, are using this utility.
- To discontinue the log at the console, use the command **`system log stop`.**

When you exit Telnet, you automatically stop any logging programs running in that session.

Note: History Log is preserved across reboots but not across power outages or power down.

Using LEDs

Most hardware problems can be easily diagnosed and solved by checking the LEDs on front panel of your router. Please refer to the section *Investigating Hardware Installation Problems* page 103, for related information.

How to Obtain Technical Support

Before calling Cabletron Systems Technical Support, have the following information ready:

- Router model number
- Router software version
- Date of purchase
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

How to contact Technical Support in the U.S.	Addresses / Numbers
Telephone	603-332-9400 Monday-Friday; 8 A.M. - 8 P.M. Eastern Time
E-Mail	support@ctron.com
Fax	603-337-2211
Address	Cabletron Systems 35 Industrial Way Rochester, NH 03867
Web Site	http://www.cabletron.com

Appendix A. Changing Configuration Switches

The configuration switches are located under the label CONFIG on the rear panel of the router. You might need to alter the configuration switches for:

- Upgrading software
- Troubleshooting with a qualified service representative
- Certain ISDN configurations
- Resetting the login password

Configuration Switches Settings

When you receive the router, switches 5 and 6 are set for the normal operation of the router. If these switches are not set in these positions when you receive the unit or you change the settings, reset them to continue normal operation.

Switches 1 and 2 are not operational.

The following table describes the meaning of each configuration switch when in the **up (off)** or **down (on)** position.

Configuration Switch Settings		Description
Switch 5	**UP (normal)**	Normal router operation mode
	DOWN	Maintenance mode
Switch 6	**UP (normal)**	Automatic boot
	DOWN	Manual boot

With both switches 5 and 6 in the down (on) position after the router has booted, the login password is overridden allowing a forgotten password to be re-entered.

Appendix B. Subnetwork Tables

Numbers of Users	Mask in decimal	Mask in hexadecimal	Bits in mask	Range of valid addresses
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.1 - .6
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.9 - .14
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.17 - . 22
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.25 - .30
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.33 - .38
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.41 - .46
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.49 - .54
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.57 - .62
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.65 - .70
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.73 - . 78
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.81 - .86
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.89 - .94
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.97 - .102
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.105 - .110
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.113 - .118
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.121 - .126
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.129 - .134
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.137 - .142
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.145 - .150
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.153 - .158
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.161 - .166
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.169 - .174
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.177 - .182
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.185 - .190
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.193 - .198
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.201 - .206
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.209 - .214
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.217 - .222
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.225 - .230
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.233 - .238
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.241 - .246
5 (+ 1 router)	255.255.255.248	FFFFFFF8	29	.249 - .254
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.1 - .14
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.17 - .30
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.33 - .46
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.49 - .62
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.65 - . 78
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.81 - .94
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.97 - .110
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.113 - .126
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.129 - .142
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.145 - .158
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.161 - .174
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.177 - .190
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.193 - .206
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.209 - .222
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.225 - .238
13 (+ 1 router)	255.255.255.240	FFFFFFF0	28	.241 - .254
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.1 - .30
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.33 - .62
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.65 - .94
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.97 - .126
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.129 - .158
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.161 - .190
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.193 - .222
29 (+ 1 router)	255.255.255.224	FFFFFFE0	27	.225 - .254
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.1 - .62
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.65 - .126
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.129 - .190
61 (+ 1 router)	255.255.255.192	FFFFFFC0	26	.193 - .254
125 (+ 1 router)	255.255.255.128	FFFFFF80	25	.1 - .126
125 (+ 1 router)	255.255.255.128	FFFFFF80	25	.129 - .254
254 (+ 1 router)	255.255.255.0	FFFFFF00	24	.1 - .254

Note 1: the router should be the lowest address in the given range.
Note 2: the mask 255.255.255.252 is legal, but it only provides for 2 addresses.

Appendix C. Network Information Worksheets

To configure the target router, you need to fill out:

- One target router chart for the target router and….
- One remote router chart for each remote router to be entered into the remote router database

If you are setting up both ends of the network:

You will need a mirror image of the information listed below for configuring the router on the other end of the ISDN link.

You will find the Network Information Worksheets for the Target Router, the Remote Router, and Bridging and Routing Controls on the following pages.

TARGET ROUTER: ……		
Configuration Section	**Item**	**Your Setting**
System Settings	Router Name	……
	Message	……..
System Settings Authentic. Password	Dial Authentication Password	……
System Settings Ethernet IP Address	Ethernet IP Address	……
	Subnet Mask	……
System Settings Ethernet IPX Network #	Ethernet IPX Network Number	……
ISDN Settings ISDN Switch	ISDN SPID #1	……
	ISDN SPID #2	……
	ISDN DN #1	……
	ISDN DN #2	……
	ISDN Switch Type	……
ISDN Settings DHCP Settings	Use defaults, but add:	
	DNS Domain Name	……
	DNS Server	…….
	WINS Server Address	……

REMOTE ROUTER: …… **Note: One chart for each remote router in the remote router database**		
Configuration Section	**Item**	**Setting**
Remote Routers Dial Settings	ISDN Phone #1, Phone #2 Inactivity timeout Maximum Links Minimum Links Utilization Threshold Bandwidth Direction	……. …….. …….. …….. …….. ……..
Remote Routers Security	Minimum Authentication Remote Router's Password	…… ……
Remote Routers Bridging	Bridging On/Off Spanning Tree On/Off	…… ……
Remote Routers TCP/IP Route Addresses	Remote Network's.IP Addresses, Masks, Metrics In Advanced: Source WAN IP Addr., mask* Remote WAN IP Address and Mask* IP RIP Protocol Options	…… …… …… ……
Remote Routers IPX Routes	IPX Routes: Network Number, Hop Count, Ticks	……
Remote Routers IPX SAPs	SAPs: Server Name, Server Type, Network Number, Node Number and Sockets WAN Network Number	…… ……

Used only in PPP numbered mode of addressing

BRIDGING AND ROUTING CONTROLS		
Configuration Section	**Item**	**Setting**
Bridging/ Routing	Default Remote Bridging Destination	…….
	TCP/IP Routing On/Off	…….
	Internet Firewall On/Off	…….
	IPX Routing On/Off	…….

Appendix D. Accessing the Command Line Interface (CLI)

Why use the Command Line Interface?

You will need to connect the router to the PC in order to access the Command Line Interface when Configuration Manager (CM, user-friendly configuration software) is not compatible with certain platforms, cannot be used.for complex configuration tasks, or if you initially experience trouble connecting to the router.

Non-Windows users have to use the CLI; Windows users may have to rely on it in specific situations, as is described below.

Non-Windows platforms (Macintosh, UNIX, etc.)

The CLI is the only configuration software available to non-Windows users. It is accessed from an ASCII terminal emulation or via Telnet to the router.

It is needed to initialize the router's IP address manually and for all configuration matters.

Windows-based platforms

The CLI is used selectively for a number of situations.

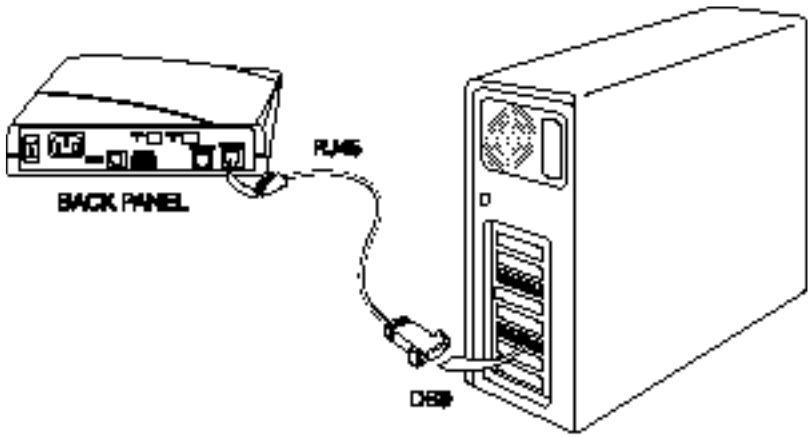
It can be accessed from within the CM or independently of it. It is specifically needed to:

- Change an existing IP address (if doing so with a POTS router is not possible. Refer to Chapter 6, *Management Tools*) to be in the same subnetwork as the PC.
- Perform advanced configurations
- Be used by network managers as the preferred management tool (for remote software management and maintenance, and troubleshooting)

Connecting the router to the PC

You will use the following.cable and.adapter:

- One 10-foot length of unshielded twisted pair cable with RJ45 connectors on either end. This cable has a green label marked "**Console**".
- One RJ45 to DB9 adapter (console port to PC)



Instructions

1. Plug the RJ45 connector at one end of the cable into the RJ45 jack marked **console** on the back panel of the router.
2. If you are connecting directly to a workstation, attach the DB9 adapter to the other end of the cable and connect that end to your workstation.

Note: Pinouts for the RJ45 connector are provided in the Quick Start Guide.

Accessing the Command Line Interface

The Command Line Interface is available at all times once you have installed the router's hardware, connected the PC with a terminal emulation session (or ASCII) session, and powered the unit on. For specifics regarding the CLI commands, refer to *Command Line Interface* guide (provided on diskette 3).

Instructions

To open a terminal window emulation program under Windows:

1. Click the **Start** button located on your PC desktop.
2. Click **Programs, Accessories**, and **Terminal.**
3. Assign the communications port connected to the console.
4. Set the terminal communications settings to the following configuration parameters:
    - 9600 bits per second
    - 8 bits
    - No parity
    - XON/XOFF support
    - 1 stop bit

To open a terminal window emulation from within Configuration Manager:

Use of Configuration Manager's Terminal Window is suitable for advanced configuration and file management. The communications settings are the same as described above.

1. Click **Tools.**
2. Click **Terminal Window.** You now have the ability to select a command using the **Commands** Menu function.

To open a terminal window emulation in a Macintosh or UNIX environment:

Refer to your system documentation to determine which appropriate communications programs to use to communicate with the router's emulation mode.

To access the terminal window via Telnet:

1. The PC address and the router address have to be in the same subnetwork.

   Ex: Router address is: 192.168.254.254
   PC address is: 192.168.254.253

2. Click the **Start** button located on your PC desktop, click **Windows Explorer**, **Windows**, and **TELNET.EXE**.

3. Select **Connect** and **Remote System** from the menu.

4. In the **Connect** window, enter the router's IP address. Click **Connect**.

Glossary

10Base-T
IEEE 802.3 standard for the use of Ethernet LAN technology over unshielded twisted pair wiring, running at 10 Mbps.

ARP
Address Resolution Protocol. An Internet protocol used to bind an IP address to Ethernet/802.3 addresses.

ASCII
American Standard Code for Information Interchange. 8-bit code for character representation.

AUI
Access Unit Interface. An IEEE 802.3 transceiver cable connecting the networked device (such as a router) to the MAU (Media Access Unit).

B-Channel
In ISDN, a full-duplex, 64 Kbps channel used for sending user data.

Bandwidth-on-Demand
Feature providing the capability of adjusting the bandwidth (opening or closing multiple B-channels) when the load in traffic increases or decreases.

BRI
Basic Rate Interface. The ISDN interface providing two 64 Kbps B-channels for voice, data and video transmission and one 16 Kbps D-channel for signaling and data transmission.

Bridge
A device that segments network traffic. A bridge maintains a list of each segment's nodes and only traffic destined for a node on the adjacent segment is passed across the bridge. A bridge operates at Layer 2 of the OSI reference model.

CHAP
Challenge Handshake Authentication Protocol. A security protocol supported under Point-to-Point Pprotocol (PPP) used to prevent unauthorized access to devices and remote networks. Uses encryption of password, device names, and random number generation.

Console
Device used by the network administrator to configure and monitor the router. The console employs an RS232 interface. Configuration Manager and Command Line Interface are used on the console.

D-Channel
In ISDN, a full-duplex 16 Kbps channel used for link setup.

DCE
Data Communicating Equipment. Equipment used within a network to transfer data from source to destination such as modems.

Data Compression
Techniques used to reduce the number of bits transferred across the communication links that represent the actual data bits. Compression is used to optimize use of WAN links and speed data transmission.

Dial-on-Demand
Dial-up WAN resources are accessed only when remote access is required and released as soon as the resource is no longer needed.

DN
Your ISDN provider (your Telco) assigns you Directory Numbers when your ISDN services are first installed. DNs are used to identify the ISDN line. Each DN is assigned for each B-channel of the ISDN line. In North America, a DN is typically a 10-digit number (Ex: 408-555-1234).

DTE
Data Terminating Equipment. DTE refers to equipment used in a network as the data source and/or destination, such as computers.

DTR
Data Terminal Ready. RS232 signal used for indicating to the DCE the readiness to transmit and receive data.

Dynamic IP Address
IP address that is assigned by the Internet provider and which may change with each connection.

EtherTalk
AppleTalk protocols running on Ethernet.

Filter
Feature to control the flow of data based on protocol or bridge information. Filters can be specific to allow data through or prevent transmission.

Firewall
A combination of techniques used to protect one network from unknown networks and users on the outside. Firewalls can filter or block traffic and act as a management and network security point where all traffic can be scrutinized.

GUI
Graphical User Interface. It allows to communicate with the computer through pull-down menus and icons.

Hop Count
Represents the number of routers in a network through which the data packet has to pass to get to its destination.

In-band Signaling
Transmission within the frequency range used for data transmission; i.e., results in use of bandwidth normally reserved for data.

IP address
Internet Address. A 32-bit address assigned to devices that participate in a network using TCP/IP. An IP address consists of four octets separated with periods defining network, optional subnetwork, and host sections.

IPX (Internet Packet Exchange)
A network layer protocol developed by Novell and used in NetWare and other networks.

ISDN
Integrated Services Digital Network. Digital transmission standard defining communication protocols permitting telephone networks to carry data, voice, fax, and other streams.

Leased Line
A telecommunications line between two service points leased from a communications carrier for private use, usually incurring a monthly service rate.

LEDs (Light Emitting Diodes)
Type of indicator lights on the panel of the router.

Local Area Network (LAN)
A network connecting computers over a relatively small geographic area (usually within a single campus or building).

MAC layer/address
Media Access Control layer/address defined by the IEEE 802.3 specification which defines media access including framing and error detection. Part of the OSI reference model data link layer.

Metric
An algorithm used by routers to determine the best path for transmitting packets to a remote destination based on considerations such as time, delay, cost, etc.

MODEM
Modulator/Demodulator. A device that converts digital signals to/from analog signals for transmission over analog communications lines.

Multi-Link Protocol
A protocol, defined in RFC 1717, defines a way to perform inverse multiplexing on the TCP/IP Point-to-Point Protocol (PPP); i.e., the ability to use multiple serial WAN channels for transferring one datastream. With MLP, a user can send and receive data over both B-channels in an ISDN basic-rate interface connection.

NetWare
A network operating system developed by Novell, Inc. providing shared access to files and other network services. IPX is the main protocol.

Network Layer
Layer 3 of the OSI reference model, which provides the protocol routing function.

Node
Refers to a termination point for communication links; entity that can access a network.

NT1
Network Terminator 1. Termination of the ISDN line at the end user's side of the connection.

OSI
Open System Interconnection. An international standard developed by ITU (formally CCITT) and ISO (International Standards Organization) to facilitate data networking multi-vendor interoperability. The OSI Reference Model defines seven layers, each providing specific network functions.

Packet
A piece of information sent across the network that includes a header and usually user data.

Ping
An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; used to test the accessibility of the remote node.

POTS
Plain Old Telephone Service referring to standard analog telecommunication.

PPP (Point-to-Point Protocol)
A Data Link layer protocol that provides asynchronous and synchronous connectivity between computer/network nodes. Includes standardization for security and compression negotiation.

Q.921
ISDN data link layer specification for the user-to-network interface.

Q.931
ISDN specification for call set-up and signaling on ISDN connections.

RFC
Request for Comment. Documentation describing Internet communications specifications (e.g. Telnet, TFTP). Often these RFCs are used to achieve multi-vendor interoperability during implementation.

RJ11
Standard 4-wire connectors for telephone lines.

RJ45
Standard 8-wire connectors used for ISDN lines.

Router Information Protocol
Protocols used in IP and IPX for broadcasting open path information between routers to keep routing tables current.

Routing
A network layer function which determines the path for transmitting packets through a network from source to destination.

RS-232
EIA standard specifying the physical layer interface used to connect a device to communications media.

Serialization Frames
Frames sent out by servers under IPX to check whether illegal copies of NetWare are in use on the network.

Service Advertising Protocol
Protocol used in IPX for broadcasting information about services available on the network, such as file servers, CD-ROM drives, and modem pools.

SNMP
Simple Network Management Protocol. A widely implemented Internet network management protocol that allows status monitoring, getting/setting of parameters for configuration and control of network devices, such as routers and bridges.

SPIDs
Service Profile Identifications. SPIDs, assigned by the ISDN service provider, identify the services and features that the switch provides to the ISDN device. Commonly implemented in the U.S. and Canada, the SPID is often derived from the directory number.

Split B-Channels
Each 64Kbps ISDN B-channel can be used individually for a separate data connection.

Spoofing
Spoofing is a technique used to remove poll and update service frames from WAN links while ensuring that the network continues to operate normally. Spoofing is employed to minimize dial-up line connection time.

Subnet Address
An extension of the Internet 32-bit addressing scheme which allows the separation of physical or logical networks within the single network number assigned to an organization. TCP/IP entities outside this organization have no knowledge of the internal 'subnetting'.

Subnet Mask
A 32-bit Internet protocol address mask used to identify a particular subnetwork.

TCP/IP
Transmission Control Protocol/Internet Protocol. Refers to a set of Internetworking protocols developed by the U.S. Department of Defense that define a two level layered approach for interoperability. TCP provides a connection-oriented transport layer ensuring end-to-end reliability in data

transmission. IP provides for network layer connectivity.using connectionless datagrams.

TELNET
Internet standard protocol for remote terminal emulation that allows a user to remotely log in to another device and appear as if directly connected.

Ticks
The number of ticks represents how much time the packet takes to reach the destination in units of roughly 1/20th of a second.

TFTP
Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) allowing for file transfer between computers over a network.

TPE
Twisted pair Ethernet, also known as 10 Base-T.

Transparent Bridging
Bridging technique used in Ethernet networks which allows transfer of frames across intermediate nodes using tables associating end nodes with bridging addresses. Bridges are unknown to the end nodes.

UDP
User Datagram Protocol. A connectionless protocol used to pass packets across an Internet network, requiring no handshaking between source and destination.

Watchdog Frames
Frames sent out by servers to clients, under IPX, to verify that clients are still logged on.

Wide Area Network (WAN)
A communications network that is geographically dispersed thus requiring links provided by communications carriers.

Workstation
Computer or terminal used by the systems administration or user.

Index

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W